

**ASSISTANT TERRITORIAL DE CONSERVATION DU PATRIMOINE  
ET DES BIBLIOTHÈQUES PRINCIPAL DE 1ERE CLASSE**

**EXAMEN PROFESSIONNEL D'AVANCEMENT DE GRADE**

**SESSION 2016**

**ÉPREUVE DE NOTE**

**ÉPREUVE ECRITE :**

**Rédaction d'une note à l'aide des éléments d'un dossier portant sur la spécialité au titre de laquelle le candidat concourt.**

Durée : 3 heures  
Coefficient : 1

**SPÉCIALITÉ : DOCUMENTATION**

**À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :**

- ♦ Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni signature ou paraphe.
- ♦ Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- ♦ Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- ♦ Les feuilles de brouillon ne seront en aucun cas prises en compte.

**Ce sujet comprend 24 pages**

**Il appartient au candidat de vérifier que le document comprend  
le nombre de pages indiqué**

*S'il est incomplet, en avertir le surveillant*

## **Sujet :**

Vous êtes assistant de conservation du patrimoine et des bibliothèques principal de 1ère classe au service documentation du département de X.

Un usager souhaite avoir des informations sur la circulation des informations personnelles des usagers de la collectivité.

Votre responsable de service vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, une note sur la protection des données personnelles.

## **Liste des documents :**

**Document 1 :** « L'impact du droit à l'oubli sur les services de documentation » - *Documentaliste - Sciences de l'information n° 4 - 2014 - 1 page*

**Document 2 :** « Données personnelles : quelles obligations ? » - *Documentaliste - Sciences de l'information n° 4 - 2014 - 2 pages*

**Document 3 :** « Une liberté documentaire : la libre circulation de l'information » - *Archimag n°274 - Mai 2014 - 2 pages*

**Document 4 :** « E-réputation : le droit à l'oubli sur internet » - *Archimag n° 278 - Octobre 2014 - 2 pages*

**Document 5 :** « Arrêt de la Cour de justice de l'Union européenne du 13 mai 2014 - *Google versus Agence de protection des données* - 3 pages

**Document 6** « Droit au déférencement - Interprétation commune de l'arrêt de la CJUE » - *CNIL - Consulté le 29 juin 2016 - 5 pages*

**Document 7 :** « Droit à l'oubli : la France en tête des demandes » - *lemonde.fr - 15 juillet 2015 - 2 pages*

**Document 8 :** « Droit à l'oubli mondial, une dangereuse chimère ? » - *lemonde.fr - 25 septembre 2015 - 2 pages*

**Document 9 :** « Protection des données : le Conseil se met d'accord sur une orientation générale » - *Communiqué de presse du 15 juin 2015, Conseil européen - 2 pages*

**Document 10 :** « Proposition de règlement du Parlement européen et du Conseil sur la protection des données » - 11 juin 2015 - 1 page

## **Documents reproduits avec l'autorisation du CFC**

*Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet.*

## L'impact du droit à l'oubli sur les services de documentation

[veille] La consécration d'un droit au déréférencement par la Cour de justice de l'Union européenne le 13 mai 2014 va-t-elle compliquer le travail des documentalistes ?

Les données personnelles sont partout et leur persistance sur les réseaux accroît désormais les conséquences de leur dissémination sur la vie privée des personnes concernées. La pression s'accroît donc pour reconnaître l'existence du droit à l'oubli ou, plus exactement, d'un droit au « déréférencement » dont la Cour de justice de l'Union européenne (CJUE) a récemment précisé les contours, mais uniquement dans le contexte des moteurs de recherche<sup>1</sup>.

### La consécration d'un droit à l'oubli

La Cour considère qu'une personne physique peut s'adresser directement à un moteur de recherche pour obtenir la suppression des liens vers des pages web contenant des informations portant atteinte à sa vie privée, indépendamment de tout recours contre l'éditeur de la page litigieuse et sans avoir à caractériser l'illicéité de la publication. Concrètement, la page web demeure accessible, mais elle ne figure plus dans les résultats du moteur de recherche. Elle devient par conséquent beaucoup plus difficile à trouver.

Si le déréférencement judiciaire était déjà une réalité<sup>2</sup> et qu'il est toujours possible<sup>3</sup>, la « déjuridictionnalisation » de la première phase de la procédure suscite de légitimes inquiétudes. Désormais, les moteurs de recherche sont susceptibles de déréférencer des liens vers des contenus qui ne sont pas manifestement illicites et peut-être même licites. En outre, la CJUE considère que le droit des données personnelles et le droit au respect de la vie privée « prévalent, également, en règle générale, sur [l']intérêt des internautes ». Ce doux euphémisme révèle la domination du droit des données personnelles sur la liberté d'information. Mais le moteur de recherche devra apprécier, pour chaque demande dont il est saisi, s'il peut y avoir une conciliation possible « dans des cas particuliers » qui dépendent :

- de la nature de l'information ;
- de sa sensibilité pour la vie privée ;
- ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique.

Dans ce contexte, les professionnels de l'information sont inquiets et les documentalistes redoutent les conséquences de cette atteinte à la liberté d'information.

La recommandation de la Cnil d'anonymiser des bases de données juridiques est une décision déjà ancienne<sup>4</sup> et bien assimilée par la profession ; celle-ci va devoir faire légèrement évoluer sa pratique des moteurs de recherche grand public.



Juriste, formateur et chercheur en droit des nouvelles techniques de l'information et de la communication depuis quinze ans, Julien LE CLAINCHE a travaillé plusieurs années dans une équipe de recherche de l'Institut de recherche en informatique et automatique (INRIA). Il est régulièrement consulté par les pouvoirs publics et le Parlement.

julien@droit-ntic.com

////

### Un impact limité pour la recherche d'information ?

Google a indiqué que le déréférencement était désormais appliqué pour tous ses sites dont les noms de domaine correspondent aux extensions géographiques des États membres de l'Union. Les liens restent donc notamment accessibles par le biais de « Google.com ». Néanmoins, Google redirige automatiquement ses visiteurs vers la version du site qui correspond à la localisation de leur adresse IP et seulement 5 % des visiteurs contourneraient cette redirection en utilisant l'adresse complète de la version américaine du site <https://www.google.com/?hl=en>.

Cette utilisation de la version américaine pour accéder à des pages déréférencées par Google.fr reste âprement contestée par la Cnil. En outre, une juridiction du fond<sup>5</sup> a récemment considéré que « c'est vainement que Google France sollicite [...] que l'injonction soit limitée aux seuls liens avec Google.fr, alors qu'il n'établit pas l'impossibilité de se connecter sur le territoire français en utilisant les autres terminaisons du moteur de recherche Google ». Cette extra-territorialité du droit français, qui confine à l'impérialisme juridique, risquerait fort de se heurter à un refus si les magistrats français demandaient au juge américain l'exequatur de leur décision nationale.

Ainsi, les documentalistes qui souhaitent formuler des recherches portant sur le nom patronymique d'une personne peuvent encore utiliser la version américaine de Google et la décision de la CJUE a, pour le moment, des effets limités sur la profession. ■

<sup>1</sup> CJUE, 13 mai 2014, Google Spain et Google, C-131/12, ECLI:EU:C:2014:317. L'Agencia Espanolã de Protecci3n de Datos (AEDP) a enjoint à Google Inc. et à sa filiale Google Spain de supprimer de la liste des résultats du moteur de recherche des liens pointant vers deux pages publiées en 1998 qui associaient une personne à des dettes de sécurité sociale acquittées depuis. La CJUE a confirmé l'analyse de l'autorité espagnole. Cette décision ne concerne que les moteurs de recherche et non les documentalistes.

<sup>2</sup> TGI Montpellier, Mme C. c/ Google France, 28 oct. 2010 ; TGI Paris, Max M. / Google France, Google Inc, 6 nov. 2013. [Legalls.net](http://Legalls.net)

<sup>3</sup> TGI Paris, M. et Mme X et M. Y / Google France, 16 sept. 2014. [Legalls.net](http://Legalls.net)

<sup>4</sup> Cnil, délibération n° 01-057, 29 nov. 2001 portant recommandation sur la diffusion de données personnelles sur Internet par les banques de données de jurisprudence. Doivent être anonymisés le nom et l'adresse des parties et des témoins, dans tous les jugements et arrêts accessibles sur Internet, quels que soient l'ordre ou le degré de la juridiction et la nature du contentieux.

<sup>5</sup> TGI Paris, 16 sept. 2014

////

## 2 LA DIFFUSION DE L'INFORMATION

# Données personnelles : quelles obligations ?

[ données personnelles ] **Exploiter des informations permettant d'identifier directement ou indirectement des personnes physiques impose le respect de plusieurs règles. Celles-ci sont appelées à évoluer prochainement.**

**C'**est le 21 mars 1974, avec la publication dans *Le Monde* de l'article de Philippe Boucher : « Safari ou la chasse aux Français », que le grand public a pris conscience des menaces que l'informatique pouvait faire peser sur la vie privée des citoyens. Le journaliste y dénonçait la mise en place par le ministère de l'Intérieur, dans le plus grand secret, d'un fichier de toute la population. Selon lui, un tel fichier risquait « de porter gravement atteinte aux libertés, et même à l'équilibre des pouvoirs politiques »<sup>1</sup>. Le scandale Safari a entraîné l'adoption en 1978 de la loi Informatique et libertés et la création de la Commission nationale de l'informatique et des libertés (Cnil).

Au niveau européen, la protection des données personnelles est harmonisée depuis 1995 dans le cadre d'une directive qui vise à établir un équilibre entre un niveau élevé de protection de la vie privée des personnes d'une part, et la libre circulation des données personnelles au sein de l'Union européenne d'autre part. Pour ce faire, la directive fixe des limites strictes à la collecte et à l'utilisation des données personnelles et impose la création, dans chaque État membre, d'un organisme équivalent à la Cnil.

La transposition en 2004 de cette directive a entraîné une modification de la loi française de 1978. La Cnil y a notamment perdu son droit de veto sur les traitements de l'État ; en revanche, elle a été dotée d'un pouvoir de sanction envers le secteur privé.

### Les grands principes

Les règles essentielles de la loi de 1978 demeurent en vigueur.

- **Information et consentement**

Toute personne doit être informée que les données la concernant vont faire l'objet d'un traitement informatisé et ce traitement ne peut avoir lieu qu'avec son consentement.

- **Droit d'accès, de modification et d'opposition**

Toute personne a le droit d'obtenir du responsable du traitement les données la concernant et de demander, le cas échéant, à les effacer, les rectifier ou compléter.

- **Finalité du traitement**

Un traitement de données doit avoir une finalité (c'est-à-dire un objectif) explicite et préalable ; les données recueillies ne peuvent ensuite être utilisées pour une autre finalité.

- **Qualité des données**

Les données traitées doivent être exactes, complètes et à jour.

- **Sécurité des données**

Le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données personnelles contre la destruction accidentelle ou illicite, l'altération, la diffusion ou l'accès non autorisés.

#### • Limitation de la durée de conservation

Les données ne peuvent être conservées que pendant la durée nécessaire à la finalité du traitement.

#### • Protection des données « sensibles »

Le traitement de certaines catégories de données (origine raciale, opinions politiques, philosophiques ou religieuses, santé, sexualité, condamnation pénales, etc.) fait l'objet de mesures particulières de protection. Sauf cas particuliers, ces données ne peuvent être traitées sans autorisation de la Cnil ou de la loi.

#### • Limitation de l'exportation hors de l'Union européenne

Les données personnelles ne peuvent être exportées que dans un pays garantissant un niveau comparable de protection. L'exportation est donc libre à travers toute l'Union européenne, ainsi que vers un certain nombre d'autres pays (la Suisse, le Canada, l'Argentine, la Norvège, l'Islande, la Nouvelle-Zélande, Israël). Pour une exportation de données vers un pays ne figurant pas dans cette liste (dont les États-Unis), une autorisation de la Cnil est nécessaire.

Préalablement à la mise en exploitation d'un traitement de données personnelles, la loi prévoit des procédures qui dépendent des cas. Pour l'État, le traitement peut être créé par un texte juridique avec avis consultatif de la Cnil. Pour le secteur privé, selon le degré de risque que le traitement fait peser sur la vie privée des citoyens, la loi prévoit une autorisation par la Cnil ou une simple déclaration, avec éventuellement engagement de respecter un cadre défini par celle-ci. La Cnil peut également, pour certaines catégories de traitements, décider d'une exemption de formalité.

### Quelles sanctions ?

La Cnil dispose par ailleurs d'un pouvoir de contrôle, avec droit d'accès à tous les traitements. En cas d'infraction à la loi Informatique et libertés, deux procédures sont possibles :

- une plainte devant le tribunal pénal sur la base des articles 226-16 et suivants du Code pénal, avec des sanctions pouvant aller jusqu'à 5 ans de prison et 300 000 euros d'amende ;
- une sanction administrative par la Cnil, se traduisant par un avertissement public ou 150 000 euros d'amende. La Cnil dispose également du droit d'ordonner l'arrêt du traitement en infraction.

Les jurisprudences disponibles montrent que les tribunaux prononcent le plus souvent des

amendes de quelques milliers d'euros assorties éventuellement, lorsque des services web sont en cause, des injonctions de retirer ou de rendre inaccessibles les contenus en infraction. Quant à la Cnil, ses sanctions pécuniaires sont souvent de plusieurs dizaines de milliers d'euros. Elle a infligé à Google, en janvier 2014, sa sanction maximale de 150 000 euros. Toutefois, il est évident qu'un tel montant n'est nullement significatif pour Google. Ce n'est donc pas la menace de la sanction, à son niveau actuel, qui aura un effet dissuasif.

### Des nouvelles dispositions prochainement

La Commission européenne souhaite actualiser la directive de 1995. Un projet de règlement européen a été adopté en mars 2014 par le Parlement européen. Il s'appliquerait à tout service visant les résidents européens.

Les formalités actuelles (déclarations, autorisations, etc.) seraient allégées. En revanche, le projet de règlement instaure, pour le responsable de traitement, une obligation de créer et de tenir à jour en interne toute la documentation concernant ses traitements, afin de permettre un contrôle effectif par les autorités de protection. Celles-ci seraient dotées d'un pouvoir de sanction renforcé : le montant maximum des sanctions serait porté à 100 millions

le montant maximum des sanctions serait porté à

100 millions d'euros

d'euros ou, pour les entreprises, 5 % de leur chiffre d'affaires mondial (le plus haut montant des deux). Une telle sanction serait sans doute effectivement dissuasive.

Le projet de règlement interdit aussi au responsable de traitement de remettre les données aux autorités judiciaires ou administratives d'un État hors de l'Union, même sur réquisition de celles-ci, sans y être autorisé par un accord international ou par les autorités de protection européennes. En cas de fuite de données personnelles, il oblige le responsable du traitement à avertir l'autorité de protection des données. En outre, et sauf si les données volées étaient chiffrées, le responsable devra avertir les personnes concernées au cas où la fuite risquerait de leur porter préjudice. Enfin, les associations de défense des consommateurs pourraient porter plainte au nom des personnes concernées.

Pour entrer en vigueur, ce projet de règlement doit désormais faire l'objet d'un accord avec la Commission européenne et avec le Conseil. Plusieurs mois de négociations sont encore à prévoir. ■



Polytechnicien et docteur en droit, Fabrice MATTATIA est expert en confiance numérique. Il a été pendant 2 ans le conseiller de la secrétaire d'État au numérique et enseigne actuellement à la Sorbonne et à Télécom ParisTech. Il est l'auteur de deux ouvrages publiés chez Eyrolles : *Traitement des données personnelles* en 2013 et *Loi et internet* en 2014.

1. On notera, pour mesurer l'évolution de la technologie en 40 ans, que le journaliste estimait qu'une capacité de mémoire de 2Go suffisait à mettre en péril la démocratie.

# une liberté documentaire :

## la libre circulation de l'information

### 1. quelques grands principes

#### ■ un principe de droit d'auteur

C'est un des principes fondamentaux du droit d'auteur : l'auteur n'exerce son droit de propriété que sur la formalisation de sa création, soit « *le choix ou la disposition des matières* » (art. L.112-3 CPI). Mais en revanche, les idées et les informations que son œuvre véhicule sont libres. Et ceci prévaut dans la plupart des pays du monde (Claude Colombet, *Grands principes du droit d'auteur et des droits voisins dans le monde*, Litec /Unesco, 1992, p.10).

#### ■ un principe de droit universel

Ce double principe de libre circulation des idées et des informations trouve son origine dans les diverses déclarations de droits de l'homme, comme corollaire à la liberté d'expression. C'est le cas de notre Déclaration des droits de l'homme et du citoyen du 26 août 1789. Son article 11 proclame « *La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout citoyen peut donc parler, écrire, imprimer librement (...)* ».

Suivront diverses déclarations internationales dont voici les principales :

- Déclaration universelle des droits de l'homme de l'ONU, 10 décembre 1948 : art.19 ;
- Conseil de l'Europe, Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, 4 novembre 1950 : art. 10 ;
- Charte des droits fondamentaux de l'Union

européenne, 7 décembre 2000, remplacée par celle du 12 décembre 2007, modifiée le 26 octobre 2012 : art.11 Liberté d'expression et d'information.

Toutes mentionnent « *la liberté de recevoir ou de communiquer des informations ou des idées* ».

#### ■ Jefferson et l'accès à la connaissance pour tous

Ce même double principe remonte aussi, logiquement, à l'époque où le commerce a commencé à porter sur des biens immatériels, essentiellement au tournant des XVIII<sup>e</sup> et XIX<sup>e</sup> siècles. Une des premières traces historiques apparaît sous la plume de Thomas Jefferson. Dans une lettre à Isaac McPherson du 13 août 1813, il s'opposait à la brevetabilité des idées au motif que « *Celui qui reçoit une idée de moi reçoit une instruction (entendons information) sans diminuer la mienne ; comme celui qui allume sa chandelle à la mienne reçoit la lumière sans m'obscurcir* ». Les idées et informations sont ainsi vues comme le gage d'accès à la connaissance pour tous, un point essentiel pour la défense des métiers de l'information-documentation dont c'est précisément la mission.

### 2. idée et information versus auteur

Tout professionnel de l'information-documentation connaît les obstacles posés par le droit d'auteur au traitement et à la diffusion de l'information, matière première de nos métiers. Le fait de rappeler avec force l'existence d'un droit à la libre circulation des idées et des informations conduit à conforter une liberté professionnelle. Et cela permet aussi de d'affirmer que ces

professionnels ne sont pas des *photocopieurs*, mais bien des *informateurs*, ayant leur pleine légitimité dans les missions qu'ils rendent à leurs utilisateurs.

N'y aurait-il donc pas abus de droit de la part des auteurs (en réalité des éditeurs d'information professionnelle ou scientifique) lorsqu'ils prétendent interdire de diffuser les informations et les idées qu'ils font passer? Leur prétexte étant qu'ils les auraient enchâssées dans des mots et des phrases leur appartenant.

La question n'est pas si simple et ne peut se réduire à l'opposition entre contenu (idées et informations libres) et contenant (œuvre de l'auteur). On sait combien certains articles sont rédigés de manière limpide et lumineuse tandis que d'autres, à volume d'information ou d'idées égal, sont illisibles. La qualité de l'information et des idées transmises tient donc pour une part dans la qualité de médiation de l'auteur.

### 3. un équilibre juridique entre information et droit d'auteur

Mais il conviendrait de trouver un juste équilibre entre la nécessaire circulation de l'information et la protection de la propriété intellectuelle. L'idée n'est pas qu'hypothétique et le législateur, notamment en droit français, a déjà consacré ce principe d'équilibre, au moins dans deux cas :

#### ① actes officiels et décisions de justice exclus du droit d'auteur.

Il est de tradition constante, contemporaine des premières lois révolutionnaires sur le droit d'auteur, de ne pas faire porter de droit d'auteur sur les « *actes officiels* ». Cette règle non écrite trouve son fondement dans l'adage « *Nul n'est censé*

*ignorer la loi* ». Puisque toute personne doit connaître le droit qui s'impose à lui, il est hors de question d'entraver la circulation de l'information juridique officielle par un quelconque droit de propriété. Ainsi sont hors du champ du droit d'auteur (et non comme exception à ce droit) tous les textes ayant force obligatoire. Il en est ainsi de la Constitution, des lois et règlements (décrets, arrêtés, actes réglementaires) ainsi que des textes de l'Union européenne applicables en France. On y ajoute les circulaires qui, sans s'imposer au citoyen, font autorité vis-à-vis de l'administration concernée. S'y ajoutent pour des raisons proches, les décisions de justice : nul n'est censé ignorer ce que dit le juge au nom de la loi, et par ailleurs ces décisions sont prises « au nom du peuple français ».

Ainsi, au nom de l'impératif de circulation de l'information juridique officielle, il est ici fait totalement échec au droit d'auteur.

#### ② l'exception de discours d'actualité.

Plus intéressante peut-être est cette exception au monopole d'exploitation de l'auteur. Il n'est pas douteux qu'un discours, même improvisé, soit une œuvre d'auteur protégée en tant que telle. Mais l'exception autorise, pour les discours prononcés publiquement, leur « diffusion, même intégrale, par la voie de presse ou de télédiffusion, à titre d'information d'actualité » (article L.122-5, 3<sup>e</sup>c du Code de la propriété intellectuelle). En d'autres termes, pendant le court délai que dure l'actualité (en fonction de la périodicité du support) l'auteur du discours voit son droit de propriété suspendu. Il le retrouve pleinement passé ce délai d'actualité. Ici nous avons le cas flagrant où des logiques professionnelles ou paraprofessionnelles s'opposent et se concilient par volonté de la loi : d'un côté les auteurs de discours publics et de l'autre les médias.

#### ③ pourquoi pas une exception de revue de presse d'actualité ?

Il ne serait donc pas illogique que le législateur introduise dans la loi une exception similaire, par exemple, l'exception d'actualité pour réaliser sereinement des revues de presse. Ce fut une des revendications de l'Association des professionnels de l'information et

de la documentation (ADBS) dans les années 1990, hélas abandonnée depuis lors. Et l'exception de revue de presse qui est dans la loi (article L.122-5 3<sup>e</sup> b CPI) ne vise que les revues de presse au sens de celles publiées dans la presse, écrite ou audiovisuelle, comme le démontre la jurisprudence (Cass. Crim. 30 janvier 1978).

## 4. la libre circulation de l'information en pratique

À défaut d'une telle nouvelle exception, il importe d'exploiter au maximum et avec doigté cette liberté de l'information pour assurer au mieux nos missions d'info-médiation.

### ■ réutiliser les seules idées et informations

Dans cette perspective, tout l'art du professionnel sera d'être capable de prélever les informations et les idées sans jamais toucher à l'œuvre protégée de l'auteur.

C'est ainsi que toute pratique visant à extraire des idées et informations d'une œuvre en vue de communiquer celles-ci est totalement licite, comme l'avait rappelé en partie l'affaire *Le Monde c/Microfor* (Cass. Ass. Plén. 30 octobre 1987).

### ■ les pratiques classiquement libres

Constituent ainsi des extractions licites d'information et d'idées : l'indexation (associer des mots-clés à un texte pour en caractériser les grands thèmes) ; le résumé et la synthèse, documentaire ou de presse ; ou encore la rédaction de « brèves » qui reprennent en quelques mots la substantifique moelle intellectuelle ou informationnelle d'un article professionnel ou scientifique. Ainsi se trouve réduite à un vœu pieux, sans portée juridique, l'exigence de la charte du Geste d'avril 2000, selon laquelle aucun résumé ne pourrait être rédigé sans l'accord de l'auteur du texte d'origine.

### ■ l'extraction de données brutes

La réutilisation de données brutes entre également dans le même espace de liberté. C'est ainsi que des chiffres clés de l'économie ou d'un autre secteur d'activité, des données géographiques brutes sont librement exploitables. Même si leur assemblage peut constituer un choix délibéré, l'extraction ponctuelle de données issues de ces ensembles n'est en rien interdite.

Et cela aussi lorsque la collection même de ces données est protégée par le droit des producteurs de bases de données.

### ■ la libre réutilisation des données publiques

Déjà traitée récemment, cette liberté en plein essor, dite open data, participe de cette liberté de circulation des informations. C'est si vrai que la réglementation encadrant l'ensemble pose ce principe de liberté sous réserve des droits de propriété intellectuelle ou de données protégées (données personnelles, par exemple). Mais on retrouve là le même principe de libre circulation des informations. ■

[Didier Frochot

→ [www.les-infostrategies.com](http://www.les-infostrategies.com)]

### ⊕ repères

#### à retenir

L'expression « titulaires de droits » vise les auteurs, mais surtout les intermédiaires que sont les éditeurs et producteurs. Malgré une certaine pression de leur part, la société de l'information repose sur une matière première libre et librement exploitable : l'information, ainsi que les idées. Cette matière première se trouve être celle des professionnels de l'information-documentation. Réutiliser celles-ci, les retraiter, les reformuler en vue de les transmettre ou de les diffuser autour de soi relève non seulement de la pure liberté, mais de la légitimité des métiers de l'information-documentation. ■

# e-réputation : le droit à l'oubli sur internet

Le monde médiatique s'est récemment focalisé sur les questions de « *droit à l'oubli* », à la suite du retentissant arrêt européen pris à l'encontre de Google. Concept nouveau pour nombre de journalistes, et largement galvaudé, dès le communiqué de presse de la CJUE.

## 1. le droit applicable

- 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 de ces données ;
- Charte des droits fondamentaux de l'Union européenne (dernière version 26 octobre 2012) ;
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 transposant la directive ;
- Arrêt de la Cour de justice de l'Union européenne (CJUE) du 13 mai 2014.

## 2. notion de droit à l'oubli

Le droit à l'oubli apparaît dès les premières législations de protection des données à caractère personnel, dans les années 70-80 pour la plupart des pays du monde. Il s'agit de l'obligation de ne pas conserver des données personnelles au-delà du délai nécessaire à la finalité du traitement de ces données (loi de 1978, article 6, 5°).

Par exemple, un lecteur de bibliothèque qui n'emprunte plus d'ouvrage pendant un an doit être supprimé de la base des emprunteurs de l'établissement.

## 3. finalité des lois de protection des données personnelles

Les lois sur les données à caractère personnel sont destinées protéger les citoyens contre la puissance de recoupements de l'informatique. Ainsi est-il interdit pour un État de recouper n'importe quelles informations sur ses citoyens, notamment pour s'immiscer dans sa vie privée, et au sein de celle-ci, de collecter des données dites sensibles telles que les origines ethniques ou raciales, les opinions philosophiques, politiques, religieuses, etc. Même les recoupements entre les revenus déclarés et les aides sociales reçues, pour traquer les fraudes, sont sérieusement encadrés.

## 4. internet : zone de non-droit ?

Si les autorités étatiques voient leurs pouvoirs de recoupement sérieusement encadrés et les citoyens relativement protégés, il n'en est rien sur internet, et ce sans aucune raison. Pourtant quel outil est plus puissant et plus indiscret qu'un moteur de recherche qui permet à toute personne de faire tous les recoupements d'informations possibles sur le seul nom d'un individu ?

Cette ignorance des lois des pays où les moteurs de recherche sont consultables a quelque chose de choquant. Plus choquant encore est le fait que, face au « *mythe de l'internet* » couplé à l'ânerie consistant à croire en un « *vide juridique* » sur le Net, nul ne prend conscience de cette évidence :

les moteurs de recherche multinationaux bafouent depuis l'origine les lois des pays où les libertés des citoyens sont censées être protégées, spécialement la protection de leurs données personnelles.

## 5. extension du concept : le droit à l'oubli numérique

La prise de conscience de cette situation a donc été longue. En France, le concept de droit à l'oubli numérique émerge peu à peu :

- proposition de loi « *visant à mieux garantir le droit à la vie privée à l'heure du numérique* » au Sénat (3 novembre 2009) ;
- intervention de la secrétaire d'État chargée de la prospective et du développement de l'économie numérique, Nathalie Kosciusko-Morizet, au 4<sup>e</sup> Forum de la gouvernance de l'internet, à Charm El-Cheikh, en Égypte pour une mondialisation du droit à l'oubli numérique (15-18 novembre) ;
- Alex Türk, président de la Cnil, se déclare favorable à l'inscription du droit à l'oubli dans la Constitution française le 23 novembre ;
- Nathalie Kosciusko-Morizet lance le 15 avril 2010 la plateforme ministérielle « *Prospective numérique* » pour recueillir les avis des internautes et lance le projet d'une charte du droit à l'oubli, « *engagement volontaire des acteurs du Net* », hélas peu suivie d'effets concrets.

## 6. le coup de semonce de la Cour de justice européenne

Dans ce cadre, la Cour de justice de l'Union européenne rend son arrêt du 13 mai 2014. Un ressortissant espagnol avait demandé sans succès à Google de déréférencier :

une page nuisant à sa réputation. Le désaccord entre l'agence espagnole de protection des données et Google Spain fut porté en justice et les juges espagnols posèrent à la CJUE une question d'interprétation de la directive européenne sur la protection des données personnelles.

## ■ un pavé dans la mare

Ce qui semble significatif dans cette affaire, c'est que, enkystés dans leurs habitudes de pensée, les acteurs du Net et les médias n'imaginaient pas qu'on puisse tout simplement rappeler que le droit s'applique partout, y compris sur internet.

Les magistrats de la CJUE vont se livrer à une démonstration juridique imparable dont on n'a pas fini de mesurer les conséquences. Après de longs argumentaires détaillés, la décision elle-même tient en quatre courts paragraphes qui constituent les phases d'un raisonnement d'une concision et d'une force juridique remarquables.

### ① les moteurs de recherche pratiquent des traitements de données personnelles

La Cour constate d'abord que les activités d'un moteur de recherche entrent dans le champ d'application de la directive puisqu'ils pratiquent notamment des traitements de données à caractère personnel (article 2, b) et que les exploitants de ces moteurs sont les responsables juridiques de ceux-ci (article 2, d).

### ② application de la loi européenne

Le grand « sport » de Google a toujours été de se retrancher systématiquement derrière le droit américain pour refuser de respecter le droit des pays dans lesquels le moteur est consultable, et ce au mépris évident des règles de droit international privé.

La Cour constate que la directive s'applique de par son article 4, 1, a) dès lors que la filiale d'un moteur de recherche établie sur le territoire de l'Union y fait du commerce et vise les ressortissants d'un État membre.

Ce n'est que l'application, soigneusement étayée, des règles dites de « conflits de lois dans l'espace » du droit international privé : la loi applicable à un litige est celle des personnes à protéger, et en droit pénal, la loi du pays de la victime. À cet égard, l'arrêt remet les pendules à l'heure.

### ③ obligation d'effacement

La Cour constate ensuite qu'en application des articles 12, b) et 14, a) de la directive (droits de rectification et d'opposition), l'exploitant d'un moteur est obligé de supprimer de ses résultats les liens pointant vers des pages sur lesquelles le demandeur est mentionné, même si cette mention n'a pas été supprimée de ces pages, et même si cette mention est licite.

### ④ un droit fondamental du citoyen européen

Enfin, la Cour fonde ce droit à l'effacement sur les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (droit au respect de la vie privée ; protection de ses données personnelles et principe du consentement pour publier celles-ci). Ce droit fondamental joue sans qu'il soit nécessaire d'invoquer un préjudice. Il prévaut « en principe », sur l'intérêt économique de l'exploitant du moteur et surtout sur l'intérêt du public à accéder à l'information, à moins que l'intérêt prépondérant du public ne l'emporte comme dans le cas d'une personnalité publique.

## 7. une interprétation trop restrictive des moteurs de recherche

Très vite assaillis de demandes, les deux grands moteurs ont mis en place un formulaire (Google le 29 mai, Bing le 16 juillet 2014). Mais entre le droit à l'effacement de l'intéressé qui n'a pas à prouver de préjudice et qui prime sur le droit à l'information du public et la possibilité de reconnaître un fort intérêt du public, se trouve créée une zone grise sujette à interprétation plus ou moins large dans laquelle les moteurs de recherche se sont engouffrés de manière excessive.

### ■ un filtrage des demandes abusif

Google et Bing exigent ainsi des « *explanations* » pour leur permettre de « *juger* » de l'opportunité du retrait là où l'arrêt précise qu'il s'agit d'un droit fondamental indépendant de tout préjudice. Et ces moteurs rejettent actuellement environ 50 % des demandes.

### ■ un masquage purement local en pratique peu efficace

Google n'efface les résultats que sur ses plateformes nationales des pays de l'Union. Il suffit par exemple de passer dans un autre pays pour retrouver toutes les informations indésirables... Or, les droits fondamentaux d'un citoyen européen ne sauraient différer dans leur application d'un pays à l'autre.

### ■ un droit à l'oubli en trompe-l'œil

Même depuis un État membre, on peut se connecter sur Google.com pour retrouver les informations indésirables, là où l'arrêt a posé le principe d'un retrait général.

## 8. bien maigre bilan

Les droits du citoyen européen sont en fait bafoués par un soi-disant droit à l'oubli qui reste plus que relatif malgré le rappel à l'ordre de la CJUE.

## 9. le G29 fourbit ses armes

Le groupe des autorités de protection des données des 28 États de l'UE (dit G29) prépare depuis l'été 2014 des lignes directrices pour coordonner son intervention, notamment face aux plaintes qu'elles reçoivent suite au refus de déréférencement des moteurs de recherche. La Cnil a annoncé le 18 septembre 2014 que le groupe commençait à organiser un réseau de travail entre les autorités et continuait à analyser la façon dont les moteurs se conforment à l'arrêt de la CJUE. Espérons que le résultat de cette étude – annoncé pour l'automne – débouchera à nouveau sur un rappel au respect plus exact de l'arrêt de la CJUE. Juges des contentieux opposant les citoyens aux moteurs de recherche en cas de refus de déréférencement, ces autorités contribueront de toute façon à dégager une jurisprudence régulatrice des pratiques des moteurs. ■

Didier Frochot

[→ [www.les-infostrategies.com](http://www.les-infostrategies.com)]

## DOCUMENT 5

### *Google versus Agence de protection des données*

ARRÊT DE LA COUR (grande chambre)

13 mai 2014 (\*)

«Données à caractère personnel – Protection des personnes physiques à l'égard du traitement de ces données – Directive 95/46/CE – Articles 2, 4, 12 et 14 – Champ d'application matériel et territorial – Moteurs de recherche sur Internet – Traitement des données contenues dans des sites web – Recherche, indexation et stockage de ces données – Responsabilité de l'exploitant du moteur de recherche – Établissement sur le territoire d'un État membre – Portée des obligations de cet exploitant et des droits de la personne concernée – Charte des droits fondamentaux de l'Union européenne – Articles 7 et 8»

Dans l'affaire C-131/12,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par l'Audiencia Nacional (Espagne), par décision du 27 février 2012, parvenue à la Cour le 9 mars 2012, dans la procédure

**Google Spain SL,**

**Google Inc.**

contre

**Agencia Española de Protección de Datos (AEPD),**

**Mario Costeja González,**

LA COUR (grande chambre),

composée de M. V. Skouris, président, M. K. Lenaerts, vice-président, MM. M. Ilešič (rapporteur), L. Bay Larsen, T. von Danwitz, M. Safjan, présidents de chambre, MM. J. Malenovský, E. Levits, A. Ó Caoimh, A. Arabadjiev, M<sup>mes</sup> M. Berger, A. Prechal et M. E. Jarašiūnas, juges,  
avocat général: M. N. Jääskinen,  
greffier: M<sup>me</sup> M. Ferreira, administrateur principal,  
vu la procédure écrite et à la suite de l'audience du 26 février 2013,  
considérant les observations présentées:

- pour Google Spain SL et Google Inc., par M<sup>es</sup> F. González Díaz, J. Baño Fos et B. Holles, abogados,
- pour M. Costeja González, par M<sup>e</sup> J. Muñoz Rodríguez, abogado,
- pour le gouvernement espagnol, par M. A. Rubio González, en qualité d'agent,
- pour le gouvernement hellénique, par M<sup>me</sup> E.-M. Mamouna et M. K. Boskovits, en qualité d'agents,
- pour le gouvernement italien, par M<sup>me</sup> G. Palmieri, en qualité d'agent, assistée de M. P. Gentili, avvocato dello Stato,
- pour le gouvernement autrichien, par M. G. Kunnert et M<sup>me</sup> C. Pesendorfer, en qualité d'agents,

- pour le gouvernement polonais, par MM. B. Majczyna et M. Szpunar, en qualité d’agents,
  - pour la Commission européenne, par M<sup>me</sup> I. Martínez del Peral et M. B. Martenczuk, en qualité d’agents,
- ayant entendu l’avocat général en ses conclusions à l’audience du 25 juin 2013,  
rend le présent

### Arrêt

- 1 La demande de décision préjudicielle porte sur l’interprétation des articles 2, sous b) et d), 4, paragraphe 1, sous a) et c), 12, sous b), et 14, premier alinéa, sous a), de 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 de ces données (JO L 281, p. 31), ainsi que de l’article 8 de la charte des droits fondamentaux de l’Union européenne (ci-après la «Charte»).
- 2 Cette demande a été présentée dans le cadre d’un litige opposant Google Spain SL (ci-après «Google Spain») et Google Inc. à l’Agencia Española de Protección de Datos (AEPD) (agence de protection des données, ci-après l’«AEPD») et à M. Costeja González au sujet d’une décision de cette agence faisant droit à la plainte déposée par M. Costeja González contre ces deux sociétés et ordonnant à Google Inc. d’adopter les mesures nécessaires pour retirer des données à caractère personnel concernant M. Costeja González de son index et d’empêcher l’accès à celles-ci à l’avenir.

(...)

Par ces motifs, la Cour (grande chambre) dit pour droit:

- 1) **L’article 2, sous b) et d), de 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 de ces données, doit être interprété en ce sens que, d’une part, l’activité d’un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné doit être qualifiée de «traitement de données à caractère personnel», au sens de cet article 2, sous b), lorsque ces informations contiennent des données à caractère personnel et, d’autre part, l’exploitant de ce moteur de recherche doit être considéré comme le «responsable» dudit traitement, au sens dudit article 2, sous d).**
- 2) **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.

- 3) 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 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.
- 4) Les articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46 doivent être interprétés en ce sens que, dans le cadre de l'appréciation des conditions d'application de ces dispositions, il convient notamment d'examiner si la personne concernée a un droit à ce que l'information en question 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, sans pour autant que la constatation d'un tel droit présuppose que l'inclusion de l'information en question dans cette liste cause un préjudice à cette personne. Cette dernière pouvant, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte, demander que l'information en question ne soit plus mise à la disposition du grand public du fait de son inclusion dans une telle liste de résultats, ces droits 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 accéder à ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question.

Signatures

---

\* Langue de procédure: l'espagnol.

## DOCUMENT 6

Interprétation commune de l'arrêt de la CJUE » - *CNIL*



# DROIT AU DEREFERENCMENT

## Interprétation commune de l'arrêt de la CJUE

CNIL - 8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

---

RÉPUBLIQUE FRANÇAISE

1. Que dit l'arrêt de la CJUE du 13 mai 2014 sur le droit à l'oubli ?.....	2
2. Quel rôle pour la CNIL et les autorités de protection européenne des données ? .....	2
3. Qu'est-ce que le déréférencement en pratique ?.....	2
4. Quelles garanties pour la liberté d'expression et le droit à l'information ?.....	3
5. Qui peut exercer ce droit ? .....	3
6. Comment exercer ce droit ?.....	3
7. Quelle portée territoriale donner à un déréférencement ?.....	3
8. Les moteurs de recherche doivent-ils informer du déréférencement le site à l'origine de la diffusion du contenu ? .....	4
9. Le public doit-il être informé que certains résultats n'apparaissent pas en raison des suites données à une demande de déréférencement ?.....	4

## 1. Que dit l'arrêt de la CJUE du 13 mai 2014 sur le droit à l'oubli ?

En substance, dans sa décision du 13 mai 2014 sur le droit à l'oubli, la Cour de justice de l'Union européenne (ci-après CJUE) indique que :

- les résultats affichés par les moteurs de recherche à la suite d'une requête effectuée sur la base d'un nom, sont des traitements de données à caractère personnel et doivent être distingués de ceux réalisés par les éditeurs de sites ;
- les moteurs de recherche sont responsables de ces traitements ;
- les traitements ainsi réalisés sont soumis à la législation européenne sur la protection des données dans la mesure où le moteur de recherche dispose d'un établissement sur le territoire de l'Union en charge, notamment, d'assurer la promotion et la vente d'espaces publicitaire qu'il propose ;
- les personnes disposent d'un droit à demander le déréférencement d'informations en lien avec leur identité, sous réserve de certaines conditions et notamment de l'intérêt du public à avoir accès à l'information ;

## 2. Quel rôle pour la CNIL et les autorités de protection européenne des données ?

La CNIL peut se prononcer sur les refus de déréférencement opposés par les moteurs de recherche. Ces refus peuvent également être contestés devant les juridictions compétentes.

C'est pourquoi les autorités de protection, dont la CNIL, ont mené des travaux dans le cadre du G29 sur la portée du droit au déréférencement tel que reconnu par la CJUE.

Les autorités ont ainsi adopté une grille de lecture commune de l'arrêt ainsi qu'une liste de critères destinés à les aider dans l'examen des demandes de déréférencement.

## 3. Qu'est-ce que le déréférencement en pratique ?

Il s'agit de supprimer certains résultats figurant dans la liste de ceux affichés par un moteur de recherche après une requête effectuée sur la base de données relative à une personne. 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.

#### **4. Quelles garanties pour la liberté d'expression et le droit à l'information ?**

Dans sa décision, la CJUE indique que les droits de la personne demandant un déréférencement prévalent, en principe, non seulement sur l'intérêt économique du moteur de recherche, mais également sur l'intérêt du public à accéder à ladite information. Toutefois, la Cour précise que tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans sa vie privée est justifiée par l'intérêt prépondérant du public à avoir accès à cette information.

Il appartient ainsi à la CNIL de tenir compte de l'intérêt du public à avoir accès à l'information ainsi que des circonstances de l'espèce (rôle de la personne concernée, nature de l'information...) pour de demander ou non au moteur de recherche de revenir sur sa décision de refus de déréférencement.

Lorsque l'intérêt du public à être informé est prépondérant le déréférencement n'est pas approprié.

#### **5. Qui peut exercer ce droit ?**

L'article 8 de la Charte de l'Union européenne reconnaît un droit à la protection des données à toute personne. A ce titre, toute personne résident en France peut saisir la CNIL à la suite d'un refus de déréférencement.

#### **6. Comment exercer ce droit ?**

La loi « Informatique et Libertés » s'appliquant aux moteurs de recherche, les personnes concernées peuvent contacter ceux-ci pour solliciter le déréférencement des résultats en cause, ce n'est qu'en cas de refus opposé par le moteur de recherche qu'elles peuvent saisir la CNIL. Les personnes ne sont pas obligées d'exercer au préalable une demande d'opposition auprès du site à l'origine de la diffusion du contenu ; elles peuvent directement demander le déréférencement au moteur de recherche.

#### **7. Quelle portée territoriale donner à un déréférencement ?**

Afin d'assurer l'effectivité du droit au déréférencement tel que reconnu par la CJUE, le déréférencement devra être effectif dans toutes les extensions pertinentes, y compris .com.

En effet, limiter le déréférencement aux extensions européennes des moteurs de recherche en considérant que les utilisateurs effectuent généralement des requêtes à partir des extensions nationales du moteur, ne garantit pas de manière satisfaisante le droit des personnes tel que retenu par la CJUE.

## **8. Les moteurs de recherche doivent-ils informer du déréférencement le site à l'origine de la diffusion du contenu ?**

D'une manière générale, les moteurs de recherche n'ont pas à informer du déréférencement le site à l'origine de la diffusion du contenu.

Pour autant, avant de prendre leur décision, ils peuvent être amenés à contacter les sites source dans des cas particuliers pour obtenir les informations complémentaires leur permettant de se prononcer sur la demande de déréférencement qui leur a été adressée.

Les moteurs de recherche devraient publier la liste des critères qu'ils utilisent pour instruire les demandes qui leur sont adressées ainsi que des statistiques détaillées sur leurs décisions.

## **9. Le public doit-il être informé que certains résultats n'apparaissent pas en raison des suites données à une demande de déréférencement ?**

Aucune disposition légale n'impose aux moteurs de recherche de procéder à une telle information.

Une telle pratique ne pourrait être acceptable que si cette information était donnée d'une manière qui ne laisse pas supposer qu'une personne précise a demandé le déréférencement d'un contenu le concernant.

## DOCUMENT 7

Le monde.fr – 15 juillet 2015

### Droit à l'oubli : la France en tête des demandes

Le Monde.fr | 15.07.2015 à 13h37 • Mis à jour le 15.07.2015 à 13h44 | Par Morgane Tual ([journaliste/morgane-tual](#))



En France, 224 demandes de « droit à l'oubli » étaient liées à des politiques. © Dado Ruvic / Reuters / REUTERS

Un million : c'est le nombre d'URL (*Uniform Resource Locator*, littéralement « localisateur uniforme de ressource », en français, ou adresse d'une ressource Internet) que les internautes européens ont demandé à Google de déréférencer, au nom du « droit à l'oubli », mis en place en mai 2014.

A la suite d'une décision de la Cour de justice de l'Union européenne ([/pixels/article/2014/09/23/google-condamne-au-nom-du-droit-a-l-oubli\\_4493067\\_4408996.html](#)), le moteur de recherche leur permet de remplir un formulaire en ligne ([https://support.google.com/legal/contact/lr\\_eudpa?product=websearch&hl=fr](https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr)) afin de réclamer la suppression de résultats de recherche les concernant.

Plus d'un an après le lancement de ce dispositif, Google a publié cette semaine des chiffres (<http://www.google.com/transparencyreport/removals/europeprivacy/?hl=fr>) sur le nombre de requêtes reçues. On y apprend que 283 276 demandes ont été faites, concernant précisément 1 030 182 URL. La firme américaine a accepté d'en déréférencer moins de la moitié, à savoir 41,3 %.

La France est le pays le plus demandeur, avec près de 200 000 URL concernées, suivie par l'Allemagne et la Grande-Bretagne. Ainsi 47,7 % des requêtes françaises ont été acceptées. En revanche, quand on rapporte ces requêtes au nombre d'habitants, l'Estonie est en tête, suivie du Lichtenstein et des Pays-Bas.

**Lire aussi : Comment Google applique le « droit à l'oubli » en Europe** ([/pixels/article/2015/05/14/google-precise-comment-il-applique-le-droit-a-l-oubli-impose-par-l-ue\\_4633654\\_4408996.html](#))

### Facebook, YouTube et Badoo touchés

Les sites les plus touchés par ces déréférencements sont les principaux réseaux sociaux, tels que Facebook, Twitter, Google+ ou encore YouTube. Sont également concernés les sites agrégeant des informations sur les personnes, comme ProfileEngine, Yasni, 192.com, mais aussi le site de rencontres Badoo.

Google donne des exemples, anonymes, de requêtes reçues ces derniers mois. En France, un prêtre condamné pour détention d'images pédophiles a souhaité, en vain, faire désindexer des articles sur le sujet. En Italie, une femme a pu faire retirer des articles de plus de dix ans sur le meurtre de son mari, dans lesquels son nom était mentionné. En Grande-Bretagne, un fonctionnaire a exigé le retrait d'une pétition réclamant sa démission. Google n'a pas accédé à sa demande.

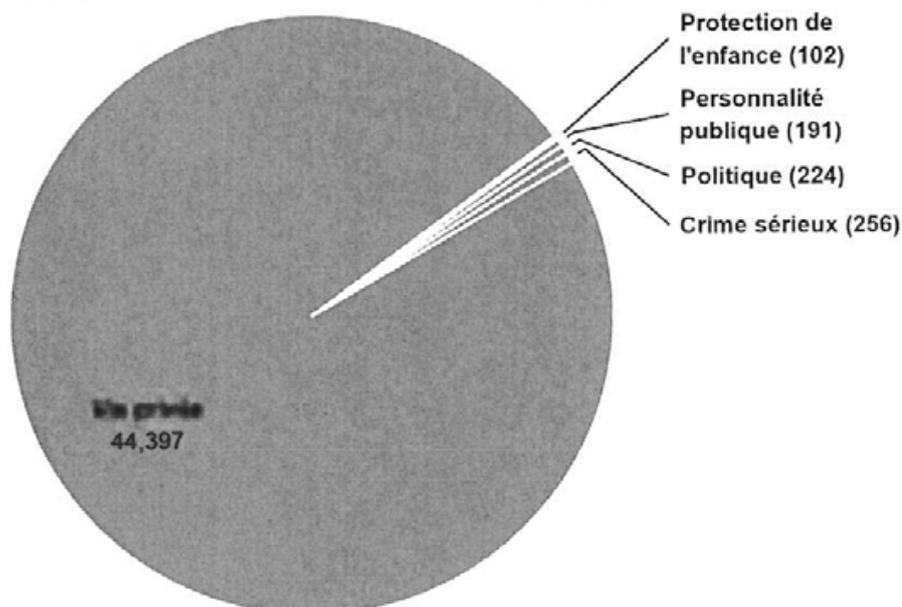
## En France, 224 demandes liées à des politiques

Toutefois, les requêtes concernant des « crimes sérieux » ou des personnalités publiques sont très marginales. C'est ce que révèle le *Guardian* ([http://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests?CMP=twf\\_technology-gdntech](http://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests?CMP=twf_technology-gdntech)) qui, en fouillant dans le code source de la page de Google présentant ces chiffres, a trouvé des données (<http://sytp.github.io/frtb/index.html>) que le géant du Web n'avait pas rendues publiques, portant sur les trois quarts des requêtes – ces données ont depuis été supprimées. On en apprend plus sur le type de requêtes effectuées, et on découvre notamment que plus de 95 % des demandes concernent des informations relatives à la vie privée, comme des photos dénudées ou d'autres contenus embarrassants.

Ce chiffre grimpe à 98,3 % en France, où les requêtes concernant les « crimes graves » n'atteignent que 0,6 %. On découvre aussi dans ces chiffres que 224 demandes en France étaient liées à des politiques, dont 66 ont été acceptées. Cent quatre-vingt-onze étaient liées à des « personnalités publiques » – chefs d'entreprises, artistes, sportifs...

## En France, la grande majorité des requêtes concerne la vie privée

Nombre de requêtes de suppression d'URL classées par type de demande.



SOURCE: GOOGLE

A noter que l'Italie est en première position sur les demandes pour « crimes grave », avec pas moins de 12 % des requêtes, et la Roumanie en tête des demandes « politiques ».

Chacune d'entre elles est examinée individuellement, et les employés de Google, épaulés par des juristes, doivent trancher. Google donne quelques précisions (<http://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=fr>) sur les critères d'acceptation :

« Lors de l'examen d'une demande, nous regardons si les résultats contiennent des informations obsolètes ou incorrectes sur la personne. Nous regardons également si les informations que nous conservons dans nos résultats de recherche sont d'intérêt public ou non, si elles sont associées à des escroqueries financières, à des fautes professionnelles, à des condamnations en justice ou aux actions publiques de représentants du gouvernement (élus ou non élus). »

## DOCUMENT 8

Le monde.fr – 25 septembre 2015

### Droit à l'oubli mondial, une dangereuse chimère ?

Le Monde.fr | 25.09.2015 à 16h28



Le moteur de recherche a demandé, en vain, à la Cnil de renoncer à lui demander d'étendre le « droit à l'oubli » au monde entier plutôt qu'à la seule Europe. AFP/Josh Edelson

Le 13 mai 2014, la Cour de justice de l'Union européenne (CJUE) consacrait le droit de demander aux moteurs de recherche de déréférencer les pages web comportant des informations inexactes, inadéquates ou excessives relatives à un individu ou portant atteinte à sa vie privée.

Cette décision répond à une forte attente sociale mais pose également la question du contrôle de proportionnalité entre le droit à l'information et le respect de la vie privée.

#### **Lire aussi : « Droit à l'oubli » : les autorités françaises rejettent la demande de Google**

([pixels/article/2015/09/21/droit-a-l-oubli-le-s-autorites-francaises-rejettent-la-demande-de-google\\_4765377\\_4408996.html](http://pixels/article/2015/09/21/droit-a-l-oubli-le-s-autorites-francaises-rejettent-la-demande-de-google_4765377_4408996.html))

Depuis, les autorités de protection des données personnelles tâchent d'interpréter cette décision pour permettre sa mise en pratique. Désormais, la Commission nationale de l'informatique et des libertés (Cnil (<http://www.cnil.fr/institution/actualite/article/article/droit-au-derferencement-rejet-du-recours-gracieux-forme-par-google-a-l-encontre-de-la-mis/>)) exige que Google élargisse copieusement le champ d'application du droit au déréférencement puisqu'elle considère que celui-ci doit être réalisé sur toutes les versions du moteur de recherche et non pas uniquement en Europe comme c'est le cas actuellement.

La Commission veut notamment éviter les détournements et les accès par d'autres versions des moteurs de recherche. Mais est-il réellement possible et souhaitable pour l'Europe d'imposer ses valeurs de protection de la vie privée au reste du monde ?

Le terme « droit au déréférencement » est mieux adapté que celui de droit à l'oubli puisque les pages demeurent en ligne, par exemple sur le site d'un journal, et qu'elles restent accessibles par l'intermédiaire des moteurs dès lors que les termes utilisés pour effectuer la recherche ne portent pas sur le nom patronymique.

Ainsi, même en Europe, le droit au déréférencement n'est pas absolu puisque les contenus demeurent toujours accessibles par d'autres biais. Dans ces conditions, pourquoi rechercher une efficacité absolue au niveau international ?

#### **Est-il possible d'imposer la conception européenne du droit à l'oubli ?**

La Cnil cherche à appréhender à travers les ordres juridiques français et européens des éléments

situés en dehors de leurs territoires. Concrètement, elle prétend contrôler sur le territoire d'États situés hors de l'Europe l'accès à l'information, peu importe que celle-ci soit licite ou non au regard des lois applicables dans ces pays.

En principe, pour qu'un État souverain applique sur son propre territoire le droit d'un autre ordre juridique, il faut qu'un accord international soit conclu. Dans le contexte des droits « économiques » tels que le droit des marques, des intérêts convergents permettent de dégager des accords. La lutte contre la pédopornographie et contre le terrorisme peut également aboutir à un consensus international.

En revanche, la conciliation de la vie privée avec d'autres libertés telles que la liberté d'expression et la liberté d'information est largement pétrie par un contexte socioculturel et des centaines d'années d'Histoire. La disparité dans l'espace du sens donné aux concepts et des modalités de leur conciliation rend peu probable la perspective d'un rapprochement des ordres juridiques à moyen terme.

## **Souhaitable ?**

En outre, la posture de la Cnil est dangereuse en ce qu'elle impose au reste du monde notre échelle de valeurs. Or, quelle serait notre réaction si demain un État, au nom de la réciprocité, venait nous imposer ses propres valeurs en demandant le déréférencement de caricatures à caractère religieux ou d'articles rédigés par des opposants aux politiques ?

Assurément, en visant les extensions non-européennes des moteurs de recherche, la Cnil prend le risque de créer un précédent fâcheux alors même que des solutions plus mesurées existent et qu'une réflexion sur la nécessité de la disparition absolue de toute trace devrait être plus présente.

Une solution est envisageable.

Selon Google, 97 % des internautes français utilisent Google.fr et seulement 3 % fréquentent la version américaine Google.com. Il serait plus proportionné de demander aux moteurs de recherche de continuer dans cette voie et de vérifier que la requête émane de France pour rediriger automatiquement l'internaute sur la version locale (.fr).

Cette redirection forcée est évidemment faillible puisqu'il suffit d'utiliser un « serveur proxy » ou un réseau privé virtuel pour la contourner. Cela représenterait néanmoins une part négligeable des internautes. Si le droit au déréférencement est une protection nécessaire, il n'est qu'une composante du droit à l'oubli. Il ne doit pas être instrumentalisé par des autorités de contrôle plus soucieuses de redorer leur blason après avoir été muselées lors des débats sur la conciliation des libertés avec la sécurité et la lutte contre le terrorisme que de trouver une solution pérenne.

Une réflexion plus large (oubli et santé, oubli et mineurs, oubli et passé pénal...) et mieux coordonnée, notamment avec le législateur (notamment européen) est donc nécessaire pour parvenir à un droit à l'oubli équilibré et protecteur.

**Julien Le Clainche (Avocat, docteur en droit)**

## DOCUMENT 9

*Communiqué de presse du 15 juin 2015, Conseil européen*

### **Protection des données: le Conseil se met d'accord sur une orientation générale**

Le 15 juin 2015, le Conseil est parvenu à une orientation générale concernant le règlement général sur la protection des données, qui établit des règles adaptées à l'ère numérique. Ce règlement a un double objectif: renforcer le niveau de protection des personnes physiques à l'égard des données à caractère personnel les concernant et accroître les débouchés commerciaux dans le marché unique numérique.

Dzintars Rasnačš, ministre letton de la justice, a déclaré: "Ce jour, nous avons fait un grand pas en avant pour nous rapprocher de l'objectif consistant à doter l'Union européenne d'un cadre modernisé et harmonisé de protection des données. Je suis particulièrement satisfait de constater que, après trois années de négociations, nous sommes finalement parvenus à un compromis sur le texte. Le nouveau règlement sur la protection des données, qui est adapté aux besoins de l'ère numérique, renforcera les droits de nos citoyens et assurera un niveau élevé de protection."

Fort de cette orientation générale, le Conseil dispose d'un accord politique sur la base duquel il peut maintenant entamer des négociations avec le Parlement européen en vue de parvenir à un accord global sur de nouvelles règles de l'UE en matière de protection des données. Un premier trilogue avec le Parlement devrait avoir lieu le 24 juin 2015.

"Je me réjouis que le Parlement européen soit disposé à entamer les négociations en trilogue dès la semaine prochaine. J'espère que nous parviendrons rapidement à l'accord final, de manière à ce que nos citoyens puissent bénéficier le plus tôt possible des avantages de la réforme", a ajouté le ministre letton de la justice Dzintars Rasnačš.

La future présidence luxembourgeoise a indiqué que, parallèlement aux négociations sur le règlement, les travaux relatifs à la directive en matière de protection des données dans le domaine répressif seraient accélérés, l'objectif étant de parvenir à une orientation générale en octobre. Le ministre luxembourgeois de la justice Felix Braz a déclaré: "Cette réforme constitue un paquet et nous avons la ferme intention de boucler le dossier avant la fin de l'année".

#### **Principaux éléments de l'accord**

##### ***Un niveau renforcé de protection des données***

Les données à caractère personnel doivent être recueillies et traitées de manière licite, dans des conditions strictes et à des fins légitimes. Les responsables du traitement (ceux qui sont chargés de traiter les données) doivent respecter des règles bien précises, comme l'obligation de recueillir le consentement sans ambiguïté de la personne concernée (la personne dont les données à caractère personnel font l'objet d'un traitement) pour pouvoir traiter ces données.

Grâce au renforcement des droits en matière de protection des données, les personnes concernées peuvent mieux maîtriser leurs données à caractère personnel:

- *un accès plus facile à leurs données;*
- des informations plus détaillées sur ce qui arrive à leurs données à caractère personnel une fois qu'elles décident de les partager: les responsables du traitement doivent offrir davantage de transparence sur la manière dont ces données sont traitées, par exemple en informant en termes simples et clairs les personnes de la politique applicable en matière de respect de la vie privée;
- un droit à l'effacement et à l'oubli numérique, qui permet à tout un chacun de demander, par exemple, qu'un fournisseur de services supprime sans délai des données à caractère personnel recueillies lorsque l'intéressé était enfant;
- un droit à la portabilité, qui permet de transmettre plus facilement des données à caractère personnel d'un fournisseur de services, par un exemple un réseau social, à un autre, ce qui permettra en outre d'accroître la concurrence entre ces fournisseurs;
- des limites à l'utilisation du "profilage", à savoir le traitement automatisé de données à caractère personnel visant à évaluer certains aspects personnels tels que le rendement au travail, la situation économique, la santé, les préférences personnelles, etc.

Afin d'améliorer les possibilités de recours, les personnes concernées pourront soumettre toute décision de leur autorité chargée de la protection des données au contrôle de leur juridiction nationale, quel que soit l'État membre dans lequel le responsable du traitement est établi.

### ***Des débouchés commerciaux accrus dans le marché unique numérique***

Un ensemble unique de règles valables dans toute l'Union et applicable aux entreprises européennes et non européennes offrant leurs services en ligne dans l'UE permettra d'éviter que des règles nationales divergentes en matière de protection de données n'entravent les échanges transfrontières de données. En outre, une coopération accrue entre les autorités de contrôle des États membres assurera une application cohérente de ces règles dans toute l'UE, ce qui créera une concurrence loyale et encouragera les entreprises, notamment les petites et moyennes, à tirer le meilleur parti du marché unique numérique.

Afin de réduire les coûts et d'offrir une sécurité juridique, dans des affaires transnationales importantes faisant intervenir plusieurs autorités de contrôle nationales, une décision de contrôle unique sera prise. Ce mécanisme de guichet unique permettra à une entreprise ayant des filiales dans plusieurs États membres de limiter ses contacts à l'autorité chargée de la protection des données de l'État membre dans lequel elle est établie.

Pour réduire les coûts de mise en conformité, les responsables du traitement peuvent, sur la base d'une évaluation du risque que comporte leur traitement de données à caractère personnel, définir des niveaux de risque et mettre en place des mesures qui tiennent compte de ces niveaux.

### ***Des outils plus nombreux et de meilleure qualité pour faire appliquer les règles en matière de protection des données***

Le renforcement de la responsabilité et de l'obligation de rendre des comptes incombant aux responsables du traitement améliorera le respect des nouvelles règles en matière de protection des données. Les responsables du traitement doivent mettre en œuvre des mesures de sécurité appropriées et veiller, sans retard injustifié, à adresser notification des violations de données à caractère personnel à l'autorité de contrôle ainsi qu'à ceux qui sont affectés de manière sensible par ces violations. Les responsables du traitement et les sous-traitants peuvent désigner dans leur organisation des délégués à la protection des données. En outre, ils peuvent être tenus de le faire, en vertu du droit de l'Union ou de la législation nationale.

Les personnes concernées ainsi que, dans certaines conditions, les organisations de protection des données peuvent introduire une réclamation ou former un recours juridictionnel dans les cas où les règles en matière de protection des données ne sont pas respectées. En outre, lorsque de tels cas sont confirmés, les responsables du traitement s'exposent à des amendes pouvant s'élever à un million d'euros ou à 2 % du chiffre d'affaires annuel mondial.

### ***Garanties concernant les transferts de données à caractère personnel en dehors de l'UE***

La protection des transferts de données à caractère personnel vers des pays tiers et à des organisations internationales est assurée grâce à des décisions constatant le caractère adéquat du niveau de protection. La Commission, avec la participation des États membres et du Parlement européen, est compétente pour décider si le niveau de protection des données offert par un pays tiers ou une organisation internationale est suffisant. Dans les cas où aucune décision de ce type n'a été prise, le transfert des données à caractère personnel ne peut intervenir que si des garanties appropriées (clauses types de protection des données, règles d'entreprise contraignantes, clauses contractuelles) ont été mises en place.

## DOCUMENT 10

**Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL**  
**Protection des données à caractère personnel: traitement et libre circulation des données**  
**(règlement général sur la protection des données)**

Extrait : « **Article 17 : Droit à l'effacement et à l'oubli numérique** »

1. Le (...) responsable du traitement est tenu d'effacer les données à caractère personnel dans les meilleurs délais, notamment en ce qui concerne les données à caractère personnel qui sont collectées lorsque la personne concernée a le statut d'enfant, et la personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant, dans les meilleurs délais, pour l'un des motifs suivants:
  - a) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées;
  - b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), (...) et il n'existe pas d'autre motif légal au traitement des données;
  - c) la personne concernée s'oppose au traitement des données à caractère personnel en vertu de l'article 19, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement des données à caractère personnel en vertu de l'article 19,
  - d) les données ont fait l'objet d'un traitement illicite;
  - e) les données doivent être effacées pour respecter une obligation légale à laquelle le responsable du traitement est soumis.
- 1 bis. En outre, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant, dans les meilleurs délais, si les données ont été collectées dans le cadre de l'offre de services de la société de l'information visés à l'article 8, paragraphe 1. (...).
2. (...).
- 2 bis. Lorsqu'il (...) a rendu publiques les données à caractère personnel et est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, en tenant compte des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, permettant d'informer les responsables qui traitent les données que la personne concernée (...) a demandé l'effacement par ces responsables de tout lien vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci.
3. Les paragraphes 1, 1 bis et 2 bis ne s'appliquent pas dans la mesure où (...) le traitement des données à caractère personnel est nécessaire:
  - a) à l'exercice du droit à la liberté d'expression et d'information ;
  - b) pour respecter une obligation légale qui requiert le traitement de données à caractère personnel prévue par le droit de l'Union ou par la législation d'un État membre à laquelle le responsable du traitement est soumis ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
  - c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et h ter), ainsi qu'à l'article 9, paragraphe 4 ;
  - d) à des fins d'archivage dans l'intérêt général ou à des fins scientifiques, statistiques et historiques (...), conformément à l'article 83 ;
  - e) (...)
  - f) (...)
  - g) à la constatation, à l'exercice ou à la défense de droits en justice.
4. (...)
5. (...)

*Bruxelles, le 11 juin 2015, Note au Conseil, N° doc. préc.: 9398, Objet: Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) - Préparation d'une orientation générale*