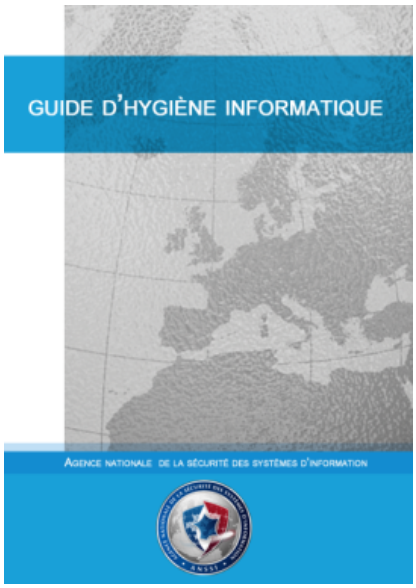
Les guides des bonnes pratiques de l’Anssi en matière de sécurité informatique | Denis JACOPINI



Les guides des bonnes pratiques de l’Anssi en matière de sécurité informatique

Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les mots-clés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

LISTE DES GUIDES DISPONIBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie – les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios – expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique… comment le sécuriser ?
- pssi – guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi – guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip – guide d'intégration de la sécurité des systèmes d'information dans les projets

---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

Nos ordinateurs ont-ils la mémoire courte ? Vidéo

Nos ordinateurs ont-ils la mémoire courte ? Vidéo

Que trouveront les archéologues du futur, d'ici quelques siècles ou quelques milliers d'années ? Des pierres taillées du paléolithique, des hiéroglyphes, des rouleaux de parchemins probablement, des livres peut-être.

https://www.youtube.com/watch?v=KCD1h8o7QTg
Quelles images, quels sons, quels écrits de notre société restera-t-il dans 2000 ans ? Auront-ils résisté aux épreuves du temps et aux mutations technologiques comme l'ont fait la première photo, le premier film, le premier enregistrement sonore.Mais que deviendront les milliards d'informations engrangées dans les disques durs qui se démagnétisent, et sur les CD ou DVD, qui redoutent la lumière du soleil ?[lire la suite]

Réagissez à cet article

Source : *Nos ordinateurs ont-ils la mémoire courte ?*

Découvrez tout ce que Google sait de vous

	**Découvrez tout ce que Google sait de vous**

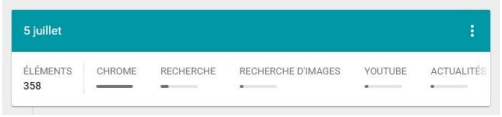
Le géant de la recherche vient d'inaugurer une nouvelle page, limpide et fonctionnelle, pour vous faciliter la vie.

La page Google Mon activité

La nouvelle page *Google Mon activité* est désormais le point de rendez-vous par excellence à l'heure de décortiquer tout ce que Google archive à votre sujet.

+ Cliquer ici pour accéder à la page Google Mon activité

Les yeux ébahis, vous découvrez minute par minute, heure par heure, jour par jour, **l'enregistrement détaillé de vos activités** au cœur des services Google.
Sont encodées vos activités et vos recherches sur: Android, Chrome, Google Maps, Recherche, Recherche d'images, Recherche de vidéos, Trajets Google Maps, YouTube.



Le 5 juillet, Google à l'affût a gardé la trace tangible de 358 activités sur notre compte Google, via le navigateur Chrome, la recherche, YouTube…PHOTO: CAPTURE D'ÉCRAN

Consulter l'historique de vos trajets

En marge de cet archivage obsessionnel, Google se fait fort d'**enregistrer vos déplacements** via la puce GPS de votre smartphone et/ou de votre tablette.
«Redécouvrez les lieux que vous avez visités et les itinéraires que vous avez empruntés dans l'historique de vos trajets», positive le moteur de recherche.

+ Cliquer ici pour consulter l'historique de vos trajets associé à votre compte Google

Les points rouges sur la carte montrent tous les endroits où Google vous a identifié grâce à la puce GPS de votre appareil mobile.PHOTO: CAPTURE D'ÉCRAN
La plate-forme pousse le vice jusqu'à présenter le classement des *«lieux que vous fréquentez le plus souvent»*.

Effacer des données archivées

Vous souhaitez éclaircir, voire supprimer, cet archivage effréné de vos données personnelles?
Soulagement, la page *Google Mon activité* vous en laisse la possibilité, sans vous mettre des bâtons dans les roues.
À partir de la page *Google Mon activité*, cliquez sur *Supprimer des activités par*

La section Supprimer des activités par vous permettra d'effacer partiellement ou totalement les données personnelles archivées par Google.PHOTO: CAPTURE D'ÉCRAN

Limiter la collecte des données

Une fois le nettoyage de printemps bouclé, libre à vous de **limiter partiellement ou autant que possible la collecte des données personnelles**.
Prenez à nouveau la direction de la page *Google Mon activité*.
Cliquez sur *Commandes relatives à l'activité*

Via la section Commandes relatives à l'activité, vous pourrez brider l'espionnage de Google.PHOTO: CAPTURE D'ÉCRAN

Réagissez à cet article

Source : *Voici comment consulter tout ce que Google sait de*

Google fait semblant de ne rien comprendre à ce qu’exige la Cnil

Google fait semblant de ne rien comprendre à ce qu’exige la Cnil

Source : *Droit à l’oubli : Comment Google feint de ne rien comprendre à ce qu’exige la Cnil – Politique – Numerama*

Droit à l’oubli : Google dévoile les domaines les plus affectés

Droit à l’oubli : Google dévoile les domaines les plus affectés

---

Google a publié un nouveau rapport concernant ses travaux dans le cadre du droit à l'oubli. Celui-ci met en évidence les noms de domaine principalement concernés.

En mai 2014, la Cour de justice de l'Union européenne avait ordonné aux moteurs de recherche en Europe de publier un formulaire de droit à l'oubli.
Ce dernier permet à un individu, ou une entreprise, de gérer sa réputation sur Internet en demandant au moteur de retirer des liens pointant vers certaines pages désuètes, ou qui affectent son image ou sa vie privée.
Au total, Google explique avoir reçu 348 085 requêtes de la part des internautes, lesquelles portent au total sur 1 234 092 liens. Le géant de la recherche affirme avoir accepté 42% de ces demandes.

En France, 73 399 formulaires ont été remplis portant sur 246 158 URL.

Google en a profité pour partager les noms de domaine qui reviennent le plus souvent au travers du formulaire de droit à l'oubli :
www.facebook.com (10220 liens supprimés)
profilengine.com (7986 liens supprimés)
groups.google.com (6764 liens supprimés)
www.youtube.com (5364 liens supprimés)
www.badoo.com (4428 liens supprimés)
plus.google.com (4134 liens supprimés)
annuaire.118712.fr (3930 liens supprimés)
www.twitter.com (3879 liens supprimés)
www.wherevent.com (3465 liens supprimés)
www.192.com (3083 liens supprimés)

Ces noms de domaine compteraient pour 9% de l'ensemble des requêtes reçues par Google.

Réagissez à cet article
Source : http://pro.clubic.com/entreprises/google/actualite-787400-droit-oublie-google-domaines-affectes.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1262345739##pid=22889469

Droit à l'oubli : mode d'emploi pour demander la suppression de contenu ou photo | Le Net Expert Informatique

Droit à l'oubli : mode d'emploi pour demander la suppression de contenu ou photo

Comment demander la suppression d'un résultat de recherche Google, concernant une personne physique, qui enfreint le droit au respect de la vie privée.

Vous êtes victime d'une atteinte à votre réputation sur internet, d'une atteinte à votre image (par la publication de photos compromettantes ou tendancieuses), ou vous vous voulez faire supprimer des informations personnelles vous concernant des résultats de recherche de Google (par exemple le fait que vous avez eu une grave maladie, tel qu'un cancer, afin d'obtenir plus facilement une assurance de prêt immobilier). Voici la démarche à suivre.

Conformément à la décision de la Cour de justice de l'Union européenne du 13 mai 2014 (n°C-131/1), l'internaute français peut désormais signaler au moteur de recherche Google – qui concentre à lui seul 90% des requêtes faites sur le web – une demande de suppression d'un résultat de recherche qui contient à son égard des propos diffamations, inexacts, mensongers ou encore des informations confidentielles et personnelles sans son accord. C'est une obligation fondée sur le droit au respect de la vie privée, y compris lorsque cela concerne un compte Facebook.

En Europe, pour exercer le droit à l'oubli, il convient de s'adresser directement à Google, mais la CNIL peut aussi intervenir après un dépôt de plainte.

Toutefois, en juillet 2015, Google a fait savoir qu'il refusait d'étendre le droit à l'oubli aux noms de domaine dont l'extension est en « .com », c'est-à-dire la grande majorité des sites internet, déplore la CNIL ! Sur le blog européen du groupe, le responsable des questions de vie privée chez Google explique que le droit à l'oubli n'a pas à être appliqué à l'échelle globale, privant ainsi des centaines d'internautes français de leur droit.

Lire la suite….

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.net-iris.fr/veille-juridique/actualite/33376/droit-a-oubli-mode-emploi-pour-demander-la-suppression-de-contenu-ou-photo.php
Par Carole Girard-Oppici,

Protection des données personnelles : les entreprises bel et bien contraintes | Le Net Expert Informatique

Protection des données personnelles : les entreprises bel et bien contraintes

Pensée pour protéger le citoyen, la loi Informatique et libertés est de plus en plus détournée de son objectif premier. Tant par les salariés que par les entreprises elles-mêmes, qui n'hésitent plus à s'en servir comme arme concurrentielle. L'analyse de l'avocat François Coupez.

La protection des données à caractère personnel est née en France avec la loi du 6 janvier 1978 dite « Informatique et libertés ». Le texte a été modifié en 2004 (à la suite de la directive européenne 95/46), et il est destiné à l'être à nouveau par le projet de loi sur le numérique annoncé en grande pompe depuis deux ans maintenant… avant d'être de toute façon complètement remplacé par un projet de règlement européen (http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do%3Freference=2012/0011(COD)%26l=fr) encore en discussion qui unifiera en 2017 ou 2018 le droit de tous les pays de l'Union européenne sur le sujet.

Si ces différents projets visent à accroître de façon très importante les sanctions financières, ils ont également pour but de permettre une application plus efficace des règles (droit à l'oubli numérique/au déréférencement, co-responsabilité des sous-traitants, etc.). Mais en parallèle, on constate depuis quelques années le développement d'une véritable instrumentalisation de cette protection légale, aux règles extrêmement formelles et aux impacts potentiellement dévastateurs[1] sur l'image des entreprises prises en faute.

Salariés et clients, quand le pouvoir change de camp

Historiquement, la CNIL a eu l'occasion d'appliquer les principes de la loi « Informatique et libertés » dans plusieurs domaines, avec la plupart du temps deux points communs : d'une part la protection des clients contre l'utilisation qui serait faite de leurs données en contradiction avec les règles applicables et, d'autre part, la protection des salariés dans des hypothèses de surveillance abusive, de discrimination ou de mode d'évaluation des performances illicites.
Dans les deux cas, l'action de la CNIL conduit souvent l'entreprise fautive à revoir beaucoup plus globalement l'ensemble de ses processus et leur conformité.
Or les difficultés pratiques concernant le respect de cette réglementation pour l'entreprise ne doivent pas être sous-estimées. Elles tiennent tant à son formalisme qu'à ses conditions d'application, étant entendu que les traitements de ce type de données se développent de façon exponentielle avec la transformation numérique. De plus, l'entreprise, confrontée à un lacis réglementaire croissant et dans tous les domaines, alloue parfois ses ressources pour se mettre en conformité en fonction de l'urgence, ou du risque réel de sanction. Les entreprises ne peuvent ainsi pas toujours prétendre réussir un sans-faute en matière de protection des données personnelles… et en sont pleinement conscientes.
En parallèle, un phénomène se développe depuis quelques années, à un point tel qu'il se généralise. Sentant la faille, des clients ou des salariés bien informés n'hésitent plus à l'utiliser, non pour faire valoir leurs droits en la matière, mais pour faire pression dans le cadre d'un contentieux ou d'une revendication autre. La réglementation devient alors un simple prétexte destiné à faire plier son opposant.
Concernant le cas des clients, cela concerne souvent les entreprises disposant de nombreux points de contact avec la clientèle (et disposant de nombreux conseillers clientèles, etc.). Dans les grands réseaux, il est toujours plus difficile de faire respecter à tous les salariés en contact avec la clientèle les règles de base (notamment concernant la zone de « bloc-note » ou de note en champ libre sur les fiches clients, propices à tous les excès), ce qui multiplie les hypothèses de manquements ;
Quant aux salariés, il est de plus en plus fréquent qu'ils fassent jouer leurs droits en la matière. Par exemple, l'une des pratiques les plus fréquentes est de systématiquement avoir recours au droit d'accès aux données personnelles que leur employeur collecte sur eux, lorsque le contrat de travail arrive précocement à son terme, ou que les deux parties se retrouvent aux Prud'hommes. La pratique montre ainsi que, sur l'ensemble des personnes pouvant faire valoir leur droit d'accès dans le cas de traitements réalisés par une entreprise, près de 75% des demandes proviennent de l'interne et donc des salariés. Ainsi, il n'y a qu'à regarder la jurisprudence en droit social ces dernières années pour s'apercevoir qu'il est devenu aussi courant d'alléguer un traitement de données personnelles contraire à la loi, et donc de l'illicéité du moyen de preuve opposé à un salarié, que d'en appeler aux pages Facebook en matière de divorce. Un exemple récent nous vient de l'arrêt de la Cour d'appel de Rouen rendu le 12 mai 2015 qui invalide les preuves concernant d'une part un système de badgeage (pas d'information du comité d'entreprise) et d'autre part un logiciel permettant de contrôler les horaires des salariés (pas de formalités CNIL) : le licenciement est ainsi considéré comme étant sans cause réelle ni sérieuse.

Maintenant les contentieux… entre entreprises ?

Ce qui est plus marquant encore, c'est que ce phénomène est en passe de gagner les relations entre entreprises.
Alors que l'on s'attend à ce que ce soit la victime (client, salarié, etc.) qui fasse valoir les droits qui lui sont reconnus, les tribunaux sont en effet saisis de façon croissante de manquements à cette réglementation allégués par… des sociétés concurrentes.
Pour mettre fin à un partenariat commercial, annuler une vente, tenter de prouver une rupture abusive des relations commerciales ou empêcher un concurrent de commercialiser un service innovant, les hypothèses se multiplient dans lesquelles des tribunaux de tout type sont confrontés à cette situation.

En voici quelques exemples :

le 25 juin 2013, la Cour de cassation a rendu une décision conduisant à l'annulation de la vente d'un fichier de clients informatisé. Dans cette affaire, les associés d'une entreprise avaient vendu pour 46 000 € le seul fichier des clients de l'entreprise, fort de 6 000 clients référencés depuis 1946. Or pour l'acheteur ayant utilisé quelques semaines cette base, celle-ci était une coquille vide de 1 950 clients actifs seulement. Il en demandait donc le remboursement… qu'il obtint : pour la Cour de cassation, l'absence du respect des formalités CNIL rend toute commercialisation du fichier impossible, la vente ayant nécessairement un objet illicite.
À la suite d'une décision de la CNIL du 8 septembre 2011 autorisant pour la première fois une entreprise à traiter pour des raisons commerciales le numéro NIR (aussi appelé « numéro de sécurité sociale »), une entreprise concurrente a formé un recours considérant que l'interprétation était contestable au sens de la loi Informatique et libertés et qu'elle conduisait à un avantage concurrentiel injustifié. C'était le premier recours intenté à l'encontre d'une décision d'autorisation, alors qu'en général – et logiquement – les recours sont formés en cas de refus de la CNIL. Or, le Conseil d'État, s'il a confirmé la décision de la CNIL le 26 mai 2014, a surtout reconnu le droit à agir de la société concurrente dans cette affaire (voir, à ce sujet, l'excellent article de Guillaume Desgens-Pasanau dans Expertises N° 397 de Décembre 2014: « Données personnelles : ouverture de l'usage du NIR au secteur privé »).
Dans une affaire récente de rupture abusive alléguée de relations commerciales, la société se plaignant de la rupture (société B) proposait à l'autre société (A) de numériser pour elle des documents dans lesquels figuraient des données personnelles, et d'effectuer cette prestation depuis le Vietnam. La société A aurait donc dû demander l'autorisation de la CNIL du fait des flux de données vers ce pays, ce qu'elle n'a pas fait. Inaction qui, pour la société B, constitue un élément de preuve que la société A ne croyait en réalité pas au projet et ne comptait pas sérieusement contracter avec elle. La Cour d'appel de Paris toutefois, pour des raisons de défaut de preuve, n'a pas suivi cette analyse et a considéré le 10 avril 2015 qu'il n'y avait pas de rupture abusive.

Le grand classique des contentieux de demain ?

On le voit à travers ces quelques exemples jurisprudentiels récents, le phénomène va croissant. Il est surtout appelé à prendre encore de l'ampleur avec le futur projet de règlement européen, qui conduit à remplacer les formalités préalables par un contrôle constant de conformité et oblige donc à documenter la façon dont les traitements sont opérés à toutes les étapes. Or toutes ces informations forment un vivier de preuves de ce qui a été fait (ou pas), destinées au régulateur… et qui pourraient facilement être utilisées par une société concurrente dans le cadre d'un procès.
Plus globalement, les entreprises doivent prendre conscience de cette évolution et en saisir toutes les opportunités, mais également tous les risques : il semble logique que les études de risque, réalisées préalablement à la mise en œuvre de traitement de données à caractère personnel, aient également à prendre en compte cette nouvelle donne…

A terme en effet, en cas de contentieux et dès que l'on parlera de près ou de loin de données, la vérification de la licéité des traitements de données personnelles de l'entreprise adverse pourrait devenir un préalable aussi convenu que la vérification des pouvoirs du signataire d'un acte.

Si cette évolution peut paraître critiquable car compliquant encore les dossiers en justice, elle est malgré tout le signe que la réglementation sur les données personnelles s'ancre profondément dans les habitudes. Un réel progrès, et qui n'était pas chose évidente il y a encore quelques années…

[1] Certes, 17 textes pénaux prévoient une sanction de 5 ans d'emprisonnement et de 1 500 000 € d'amende pour les entreprises qui enfreindraient les règles en la matière, mais les applications jurisprudentielles sont rarissimes. Les sanctions de la CNIL sont quant à elles beaucoup plus fréquentes, avec des montants financiers pour le moment limités à 150 000 € (le double en cas de récidive), seul Google inc. ayant été condamné à une telle peine. Leur efficacité est fortement renforcée par leur publication (fort effet d'image sur les grandes entreprises).

Source : http://www.silicon.fr/protection-donnees-personnelles-loi-instrumentalisee-116895.html
Par François Coupez, Avocat à la Cour, Associé du cabinet ATIPIC Avocat et titulaire du certificat de spécialisation en droit des nouvelles technologies

---

L'e-réputation des sociétés à l'épreuve d'Internet | Le Net Expert Informatique

L'e-réputation des sociétés à l'épreuve d'Internet

A l'heure où Internet permet aux consommateurs de se forger une opinion sur n'importe quel produit ou service, il est capital pour toute entreprise, particulièrement celles exerçant une activité via internet, de bénéficier d'une bonne e-réputation.
Parmi la multitude d'avis de consommateurs peuvent se cacher des messages diffamatoires causant des préjudices sérieux à la réputation des entreprises. Lorsque ces dernières les découvrent il peut être déjà trop tard pour agir.

Antérieurement à tout achat, les consommateurs normalement diligents effectuent des recherches sur les produits ou services qu'ils envisagent d'acheter. Leurs recherches se tournent alors vers des forums de consommateurs qui sont le plus souvent hébergés par des associations pour la défense de consommateurs. Ces forums sont mis en place afin que les consommateurs puissent exposer leurs retours sur la prestation d'un professionnel et, dans le cas où un litige pourrait naître, de trouver une médiation avec ce dernier.
Cependant, certains messages, postés par des utilisateurs, ou par des administrateurs ou modérateurs du forum, s'apparentent à des messages malveillants dont la finalité n'est plus d'avertir le consommateur ou le professionnel d'une difficulté mais clairement de jeter l'opprobre sur un professionnel ciblé.
Face à l'anonymat désinhibiteur dont profitent les (vrais ou faux) consommateurs sur internet, les e-commerçants peuvent rapidement se retrouver victimes de diffamations à leur insu. Malheureusement, les actions contre ces types de messages s'avèrent difficiles à engager, cela dû à un cadre législatif obsolète nécessitant une adaptation aux circonstances actuelles.

I/ L'e-diffamation commerciale considérée comme un délit de presse : une action rapidement prescrite pour un préjudice continu
La diffamation, qu'elle soit faite au moyen d'internet ou non, est définie par l'article 29 de la loi du 29 Juillet 1881 relative aux délits de presse. L'article 1382 du Code civil fixant la responsabilité délictuelle est ainsi exclu au profit de la loi spéciale (Cass. 2ème civ., 10 Mars 2004, n° 09-65.35).
Elle correspond à l'allégation ou l'imputation, faite de façon publique, d'un fait précis portant atteinte à l'honneur ou à la considération d'une personne physique ou morale, déterminée ou déterminable.
Le délai de prescription pour la diffamation étant de trois mois (article 65) à compter du message diffamatoire publié, l'action en réparation s'avère difficile à engager étant donné que la société victime peut connaître des faits plusieurs mois, voire années, après la publication desdits messages. Dans ce cas, la victime sera privée de réparation bien que le message restera accessible et que son préjudice sera toujours actuel.
Ce délai pouvait trouver son intérêt dans le cas des diffamations par presse « papier » car le préjudice y était temporaire. Pour ce type de diffamation, l'article diffamatoire n'était accessible qu'aux personnes ayant acheté le journal ou magazine sur lequel il était diffusé. Ce support, une fois son délai de publication passé, devenait introuvable et le préjudice, bien que n'étant pas éteint pour autant, s'amoindrissait.
Dans ces conditions, il apparaissait juste que la responsabilité de l'auteur ne puisse pas être engagée 3 mois après la publication des propos litigieux.
Tel n'est pas le cas pour les messages de diffamation sur internet. Ceux-ci, couplés aux méthodes de référencement des moteurs de recherche, deviennent facilement accessibles lorsque le nom de la société est recherché. Les liens url ne pouvant disparaître naturellement, le préjudice sera continu tant que les messages n'auront pas été retirés. Il faudra, pour cela, passer par une procédure judiciaire si l'auteur du message, ou l'administrateur du site sur lequel il est publié, refusent de le retirer amiablement. La société diffamée peut ainsi se retrouver dans l'impossibilité de faire réparer son préjudice.
Ce préjudice a des conséquences bien plus importantes que la simple atteinte à l'honneur de la société : perte de clients potentiels et/ou habituels qui ont été dupés par les messages ou qui, dans le doute, ont préféré éviter le commerçant diffamé, perte de chiffre d'affaires, perte de confiance de la part des partenaires économiques… A terme, ce sont l'existence de la société et les emplois de ses salariés qui sont menacés.
Le préjudice causé par l'e-diffamation n'est donc pas comparable à celui causé par la diffamation prévue par la loi de 1881. Les enjeux et le caractère permanent de la publication en font toute sa particularité, soulignant l'obsolescence de la loi.

II/ L'e-diffamation commerciale émanant d'un particulier et l'abus de la liberté d'expression
La loi Hadopi du 12 Juin 2009, reprenant le système de responsabilité en cascade de la loi du 29 Juillet 1881, prévoit la responsabilité de l'auteur d'un message diffamant publié sur internet. Cette dernière intervient dans le cas où la responsabilité du directeur ou du codirecteur de la publication fait défaut.
Outre le problème d'identification de l'auteur du message, les exceptions que celui-ci peut invoquer pour écarter sa responsabilité compliquent l'action en diffamation.
L'exceptio veritatis ou exception de vérité, consacrée par l'article 35 de la loi du 29 Juillet 1881, est un fait justificatif permettant à l'auteur du message, poursuivi pour diffamation, de s'exonérer de sa responsabilité en rapportant la preuve de la véracité des faits allégués. Cette exception doit respecter la procédure de l'article 55 de la loi de 1881 disposant que le prévenu devra signifier, au ministère public ou au plaignant, les faits desquels il entend prouver la véracité, en y joignant les pièces justificatives et les informations relatives aux témoins éventuels, dans un délai de 10 jours suivant la signification de la citation.

L'exception de bonne foi est reconnue de façon constante en jurisprudence par la réunion de quatre éléments :
• la légitimité du but poursuivi (intérêt que peuvent présenter les propos divulgués au vu de l'intérêt général) ;
• l'absence d'animosité personnelle : plus généralement observée par l'absence d'intention de nuire ;
• la prudence et la mesure dans l'expression (telle que l'usage du conditionnel, de sources, etc.) ;
• le sérieux de l'enquête (recherches d'éléments pour étayer les propos, observé surtout pour les articles écrits par des journalistes professionnels).

En matière de diffamation sur internet, le juge prend en compte, d'une part, la qualité de l'auteur (simple consommateur ou journaliste professionnel), et, d'autre part, le support sur lequel le message est posté (les blogs et forums de discussions étant des espaces où l'auteur peut s'exprimer plus librement que sur un journal). Il s'en dégage une certaine clémence envers l'internaute consommateur postant un message sur un forum ou un blog.
En effet, le juge privilégiera la liberté d'expression en reconnaissant que les propos divulgués représentent un intérêt général méritant d'être protégé au détriment du préjudice causé à la société (ex : Cass. Crim, 17 Mars 2015, n° 13-85-138 : les propos s'inscrivant dans un débat d'intérêt général). La responsabilité de l'internaute, auteur du message, est alors rarement engagée.

De plus, le régime de responsabilité étant calqué sur celui du délit de presse, il faudra rechercher en premier lieu la responsabilité de l'administrateur du site sur lequel les messages diffamatoires ont été publiés. L'administrateur du site peut, par ailleurs, également invoquer les faits justificatifs précédents pour s'exonérer de sa responsabilité (pour plus de détails sur la responsabilité de l'administrateur de site : http://www.village-justice.com/articles/irresponsabilite-administrateur,19548.html).

L'intérêt de la société diffamée s'opposera toujours à la liberté d'expression et l'intérêt des consommateurs qui pèseront davantage dans la balance du juge.
Il ne s'agit pas de défendre l'un au détriment de l'autre mais d'assurer une défense effective pour la société, soumise au seul jugement de la vox populi.
Dans ce sens, l'intérêt du droit de réponse reste limité du fait de la crédibilité donnée à l'e-commerçant sur le site où il est diffamé.
Quant au « droit à l'oubli », le récent bilan de l'année 2014-2015 révèle un faible taux de réponse favorable aux demandes.

Sur les presque 250 000 demandes qu'a reçues Google, 11,2 % des demandes concernaient des atteintes à la réputation et 4 % concernaient des atteintes à l'image.
Au final, un taux de 70 % de refus des demandes se stabilise depuis Août 2014 (source : https://forget.me).

L'adaptation des lois existantes, qui a pu suffire pendant un temps, peine à englober la complexité d'Internet. Aujourd'hui, un autre problème se pose qui n'existait pas auparavant : la permanence des informations sur Internet qui devrait faire l'objet d'une loi spécifique.

Source : http://www.village-justice.com/articles/reputation-des-societes-epreuve,19698.html
Par Laurent Feldman, Avocat et Raphaël Balji

Droit à l'oubli : Où en sont

les traitements des demandes à Google 6 mois plus tard…

	**Droit à l'oubli : Où en sont les traitements des demandes à Google 6 mois plus tard…**

En juin, Google satisfaisait 57% des demandes de déréférencement (transmises par Reputation VIP). En octobre, c'est le non qui l'emporte désormais largement dans 71% des cas, ce en moyenne 26 jours après la demande.

Cela fait désormais plusieurs mois que Google a mis en ligne son formulaire permettant à un internaute européen de demander l'application de l'arrêt de la CUJE relatif au droit au déréférencement.
Spécialiste de l'e-réputation, la société Reputation VIP, au travers de Forget.me, joue ainsi le rôle d'intermédiaire entre ses clients et Google, le premier moteur de recherche en Europe et donc le plus concerné par ces requêtes.
De quoi ainsi établir des statistiques, différentes cependant de celles publiées officiellement par Google – Forget.me représente environ 5% des demandes Google selon l'éditeur. De ces données, il ressort que le moteur a manifestement industrialisé le processus de traitement des requêtes.

Plus rapide, mais plus de non au terme du traitement
La durée de traitement des demandes s'est nettement accélérée au cours des six mois écoulés. En juin, Google mettait en moyenne 56 jours pour traiter une demande de déréférencement d'URLs. En octobre selon Reputation VIP, la durée moyenne est de 26 jours.

Un autre paramètre a très significativement évolué : la nature des réponses de Google. Le rapport entre Oui et Non s'est même clairement inversé. En juin, Google apportait une réponse positive dans 57% des cas. La proportion de Oui a reculé de manière quasi continue pour tomber à 29% en octobre.
En clair sept demandes de déréférencement sur dix adressées à Google (dont 54% portent sur des atteintes à la vie privée) aboutissent à un refus de la part du moteur – qui n'est pas tenu de justifier sa décision.

Dans leur guide d'application du droit au déréférencement, les autorités de protection ont cependant demandé aux services concernés de publier « la liste des critères qu'ils utilisent », mais aussi les « statistiques détaillées sur leurs décisions. »
Par ailleurs, en cas de refus du moteur, les internautes disposent toujours de recours et peuvent notamment déposer plainte, en France, auprès de la CNIL. En fin de semaine dernière, l'autorité de protection faisait état de 110 plaintes.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/droit-a-l-oubli-google-dit-de-plus-en-plus-souvent-non-39810627.htm

Droit à l’oubli : les 13 critères dégagés par la CNIL

Droit à l’oubli : les 13 critères dégagés par la CNIL

Soucieuse de ne pas laisser Google et ses concurrents fixer eux-mêmes leurs propres conditions d'application du droit à l'oubli, la CNIL a publié une liste de 13 critères à prendre en compte dans la décision de donner ou non satisfaction à une demande de déréférencement.

Le 13 mai 2014, la Cour de Justice de l'Union Européenne (CJUE) a rendu son déjà célèbre arrêt Google Spain qui oblige Google à donner satisfaction aux internautes qui demandent la censure de résultats qui les concernent, consacrant ainsi l'existence d'un « droit à l'oubli » sur Internet. Toutefois la CJUE avait aussitôt nuancé cette obligation en prévenant Google qu'il fallait étudier les demandes au cas par cas, pour refuser les requêtes d'un individu lorsqu'il « il existe des raisons particulières, telles que le rôle joué par cette personne dans la vie publique, justifiant un intérêt prépondérant du public à avoir, dans le cadre d'une telle recherche, accès à ces informations ».

La CJUE demandait que l'appréciation soit réalisée par Google lui-même, au regard de « la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à recevoir cette information ». La cour confiait ainsi à une entreprise privée le soin d'interpréter et appliquer le droit, à la place d'un juge dont c'est le métier et la fonction.
Or en signant cet arrêt inattendu qui contredisait l'avis de son avocat général, la cour de Luxembourg a fait naître un conflit inédit d'influence entre le secteur privé et des autorités publiques. D'un côté, Google a sauté sur l'occasion pour prendre un bout de souveraineté aux Etats et affirmer sa capacité autonome à déterminer ses propres critères jurisprudentiels, en mettant sur pieds un comité consultatif privé. De l'autre côté, les CNIL européennes qui se croyaient investies du pouvoir de faire respecter le droit à l'oubli avaient immédiatement annoncé leur intention de fixer elles-mêmes des critères, qu'elles appliqueraient en dernier recours si un internaute se plaint de ne pas avoir eu satisfaction. Elles ont ainsi boudé les réunions publiques de Google, n'acceptant pas d'être doublées.

C'est donc dans cet esprit que le G29, qui réunit la CNIL et tous ses homologues européens, a publié ce jeudi une première liste de critères généraux à prendre en compte dans l'acceptation ou le refus d'une demande de droit à l'oubli. Le document (.pdf) détaille chacun des critères à l'aune de l'arrêt de la CJUE. Les voici résumés (nos commentaires en italique) :

1. **Les résultats de recherche sont-ils relatifs à une personne physique ? Le résultat apparaît-il à la suite d'une recherche effectuée à partir du nom de la personne concernée ?**
Seules les recherches du nom ou du pseudonyme d'un particulier entrent dans le champ de l'arrêt Google Spain.
2. **S'agit-il d'une personne publique ? Le plaignant joue-t-il un rôle dans la vie publique ?**
Outre la détermination de ce qu'est un « rôle dans la vie publique », La CNIL ajoute un critère supplémentaire qui est de distinguer selon que l'information elle-même est une information pertinente au regard de cette vie publique, ou s'il s'agit d'une information d'ordre purement privé.
3. **Le plaignant est-il mineur ?**
Par principe si la réponse est oui le droit à l'oubli doit être respecté, au nom de 'l'intérêt supérieur de l'enfant » consacré par la Charte des droits fondamentaux de l'Union européenne.
4. **Les données sont-elles exactes ?**
En cas d'inexactitude, le droit à l'oubli joue le rôle d'un droit brutal de rectification. C'est toutefois à l'internaute d'apporter la preuve de l'inexactitude.
5. **Les données sont-elles pertinentes et/ou excessives ?**
Plusieurs sous critères sont ici ajoutés :

– Les données sont-elles relatives à la vie professionnelle du plaignant ?
une réponse positive joue en défaveur du droit à l'oubli, qui doit être utilisé pour la protection de la vie privée)
– L'information est-elle potentiellement constitutive de diffamation, d'injure, de calomnie ou d'infractions similaires à l'encontre du plaignant ?
la réponse positive doit reposer en priorité sur une décision judiciaire qualifiant les accusations, mais un critère de « contenu excessif » peut aussi s'appliquer par la CNIL
– L'information reflète-t-elle une opinion personnelle ou s'agit-il d'un fait vérifié ?
La CNIL vise ici le déréférencement de « campagnes de dénigrement » qui pourrait être accordé, ce qui semble flirter très dangereusement avec la ligne rouge de la censure pure et simple d'une opposition politique.
6. **L'information est-elle sensible au sens de l'article 8 de la Directive 95/46/CE ?**
Le fait que la page web dont la censure est demandée contient des informations sur l'origine raciale, la religion, les opinions politiques, l'orientation sexuelle, etc., doit jouer en faveur du droit à l'oubli.
7. **L'information est-elle à jour ? L'information a-t-elle été rendue disponible plus longtemps que nécessaire pour le traitement ?**
La CNIL est ici favorable à ce qu'une information devenue obsolète puisse être supprimée, y compris (c'est un cas explicité) s'il s'agit par exemple d'une condamnation en première instance annulée en appel.
8. **Le traitement de l'information cause-t-il un préjudice au plaignant ? Les données ont-elles un impact négatif disproportionné sur la vie privée du plaignant ?**
Il s'agit d'un critère de proportionnalité. La CNIL est par exemple favorable au déréférencement de pages qui relateraient une « infraction mineure » et qui posent problème pour la recherche d'un emploi, ou celui de photos intimes.
9. **Les informations issues du moteur de recherche créent-elles un risque pour le plaignant ?**
Sont visées ici les informations telles que des coordonnées bancaires, n° de passeport, adresse personnelle, etc., qui pourraient être utilisées par des tiers à mauvais escient.
10. **Dans quel contexte l'information a-t-elle été publiée ?**
A nouveau plusieurs sous-critères :
– Le contenu a-t-il volontairement été rendu public par le plaignant ?
Contrairement à ce que l'on pourrait croire, la CNIL estime que la réponse positive joue en faveur du droit à l'oubli, car il faut respecter le fait que la personne ne souhaite plus voir référencé un contenu qu'elle avait mis en ligne. Mais l'on doute que la réponse négative puisse jouer en sa défaveur. Dès lors, est-ce vraiment un critère ?
– Le contenu devait-il être public ? Le plaignant pouvait-il raisonnablement savoir que le contenu serait rendu public ?
La mise en ligne à l'insu de la personne joue en faveur du déréférencement (ce qui rejoint notre point précédent)
11. **Le contenu a-t-il été rendu public à des fins journalistiques ?**
La CNIL refuse d'en faire véritablement un critère. Tout en reconnaissant qu'il faut « prendre en considération » le caractère journalistique de l'information dont la censure est demandée, la CNIL minimise au maximum sa portée par rapport aux autres critères.
12. **La publication de l'information répond-elle à une obligation légale ? L'auteur de la publication avait-il l'obligation de rendre cette donnée personnelle publique ?**
Si oui, le droit à l'oubli sera en principe refusé, sauf si d'autres critères priment (tels que le préjudice subi)
13. **L'information est-elle relative à une infraction pénale ?**
Si la condamnation a été effacée par l'amnistie prévue par la loi, le droit doit être systématiquement accordé. Sinon, c'est la gravité et la date de l'infraction qui entrent en considération.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.numerama.com/magazine/31424-droit-a-l-oubli-les-13-criteres-degages-par-la-cnil.html
par Guillaume Champeau