Droit au déréférencement : le G29 adopte des lignes directrices

Droit au déréférencement : le G29 adopte des lignes directrices

L'arrêt de la Cour de Justice de l'Union Européenne (CJUE) du 13 mai 2014 Google Spain SL et Google Inc. v Agencia Española de Protección de Datos (AEPD) et Mario Costeja González (C-131/12) constitue une étape importante de la protection des données personnelles au regard des traitements de données opérés par les moteurs de recherche en Europe et, plus généralement, dans le monde numérique. Il accorde en effet la possibilité aux personnes de demander aux moteurs de recherche, sous certaines conditions, le déréférencement de liens apparaissant dans les résultats de recherche effectués sur la base de leurs noms.

Le mercredi 26 novembre, les autorités européennes de protection des données réunies au sein du Groupe de l'article 29 (G29) ont adopté des lignes directrices pour assurer une application harmonisée de l'arrêt de la CJUE. Celles-ci contiennent une interprétation commune de l'arrêt ainsi que des critères que les autorités utiliseront dans le cadre de l'instruction des plaintes leur parvenant suite à des refus de déréférencement par les moteurs.
Dans son arrêt, la Cour confirme l'applicabilité de la Directive 95/46/CE aux moteurs de recherche, ceux-ci étant qualifiés de « responsables des traitements » de données personnelles qu'ils opèrent dans le contexte des activités de leurs filiales établies sur le territoire de l'Union, visant à promouvoir et vendre des espaces publicitaires sur la page des moteurs afin qu'ils soient économiquement rentables.
L'arrêt prévoit expressément que l'exercice du droit au déréférencement n'affecte que les résultats obtenus après une recherche effectuée sur la base du nom d'une personne et ne se traduit pas par la suppression du lien dans les index du moteur de recherche. Autrement dit, l'information originale sera toujours accessible en ligne en effectuant une recherche sur d'autres termes ou en consultant directement le site source.
Le G29 considère que pour donner plein effet à l'arrêt de la Cour, les décisions de déréférencement doivent être mises en oeuvre de manière à garantir effectivement la protection des droits fondamentaux des personnes et à ne pas permettre leur contournement. A cet égard, 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 l'application de ce droit de manière satisfaisante. Cela signifie donc, en pratique, le déréférencement devra être effectif sur tous les noms de domaines pertinents, y compris le nom de domaine .com.
Toute personne a droit à la protection de ses données. En pratique, les autorités seront amenées à instruire les demandes des personnes ayant clairement un lien avec l'Union européenne, c'est-à-dire des personnes citoyennes ou résidentes d'un pays membre de l'Union.
D'une manière générale, les moteurs de recherche ne doivent pas informer de manière systématique les sites sources de ce que certaines de leurs pages ne sont plus accessibles sur la base d'une requête faite sur le nom d'une personne en raison d'un déréférencement. En effet, une telle communication systématique n'a pas de base légale dans la législation européenne de protection des données.
Les lignes directrices contiennent également une liste des critères communs que les autorités de protection des données appliqueront pour traiter les plaintes qu'elles reçoivent suite à des refus de déréférencement par les moteurs de recherche. La liste contient 13 critères qui doivent être considérés comme des outils de travail flexibles qui aideront les autorités dans la prise de décision. Les critères seront appliqués au cas par cas et en accord avec les dispositions nationales applicables.
Aucun de ces critères n'est déterminant à lui seul. Chacun d'entre eux doit être appliqué à la lumière des principes établis par la Cour et en particulier de celui de « l'intérêt général du public à avoir accès à l'information ».

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

Source : http://www.newspress.fr/Communique_FR_284298_1332.aspx

Comment combattre la cyber-violence à l’école ?

Comment combattre la cyber-violence à l’école ?

La cyber-violence en milieu scolaire se développe, au collège comme au lycée. Selon une enquête du ministère de l'éducation nationale, un collégien sur cinq a déjà été la cible d'insultes, d'humiliations et de brimades par SMS ou sur les réseaux sociaux.

Catherine Blaya, professeure en sciences de l'éducation et présidente de l'Observatoire international de la violence à l'école, explique l'existence de ce phénomène et la manière de lutter contre.

Qu'est-ce que la cyber-violence ?
Catherine Blaya : La cyber-violence est une forme de harcèlement réalisé, non plus uniquement dans la cour d'école ou dans la rue, mais par le biais des nouvelles technologies et des réseaux sociaux. Il peut prendre des formes multiples : du détournement de photo à la vidéo humiliante, en passant par des brimades, des moqueries, des intimidations par SMS. La spécificité de ce harcèlement est son caractère public, amplifié par le Web, qui agit ici comme une caisse de résonance.

Avez-vous des exemples concrets de ce type de harcèlement ?
Les victimes que j'ai rencontrées ont fait état de situations diverses. Des filles prises à partie sur leur apparence physique. D'autres qui sont ostracisées par des camarades qui jalousent leur succès ou désirent briser leur popularité. Les revanches à la suite de ruptures sont nombreuses aussi, comme les humiliations pour assurer la position dominante de l'agresseur.

Les filles sont-elles plus souvent visées que les garçons ?
Elles ont 1,3 fois plus de risque d'être victimes que les garçons, car elles ont une plus grande propension à mettre en scène leur corps, en postant des photos d'elles. Cela attire les commentaires malveillants et la raillerie. Soumettre son estime de soi au regard d'autrui, c'est s'exposer au harcèlement.

Le machisme n'est-il pas la cause première ?
Bien sûr ! Un machisme auquel elles participent aussi. En critiquant leurs congénères et en utilisant le même type d'arguments que les garçons. C'est le phénomène du « slut shaming ». Elles se font, elles-mêmes, l'instrument de la domination masculine.

Pourquoi les auteurs de ces violences privilégient-ils le Web ?
Les auteurs ont besoin d'un auditoire, de spectateurs pour leur violence. Ils veulent se venger ou acquérir un statut social au sein d'un groupe. Ils cherchent donc des témoins pour faire du « buzz » et gagner des « like », afin d'asseoir leur popularité. C'est pourquoi il faut pousser les jeunes témoins à intervenir. La cyber-violence ne doit pas être banalisée. Sur les réseaux sociaux, le problème est démultiplié par un effet de viralité. Le danger supplémentaire d'Internet est que l'agresseur qui lance une rumeur sur la Toile ne peut plus la maîtriser après coup, même s'il se rétracte. Le mal est fait pour durer.

Comment réagir face aux agresseurs ?
Il ne faut pas oublier que les agresseurs sont aussi des victimes dans la plupart des cas. C'est pourquoi il est important d'expliquer aux victimes que répondre à la violence par la violence, c'est prendre le risque de devenir soi-même agresseur. Ces derniers sont souvent des jeunes en quête de popularité qui n'ont pas confiance en eux, ou sont dans une détresse psychologique. J'ai récemment eu le cas d'un jeune homme qui après une rupture difficile s'est mis à harceler son ex-compagne.

Au quotidien, comment empêcher ces violences et harcèlement ?
Il faut beaucoup informer sur le rôle primordial des témoins dans la dénonciation de ces violences. L'enquête du ministère de l'éducation nationale indique qu'un collégien sur cinq est concerné par la cyber-violence. Mais selon mes propres études, c'est plutôt 42 % des jeunes qui sont atteints au moins une fois dans l'année. Et près de la moitié d'entre eux sont à la fois victimes en ligne et dans la cour d'école. La majorité de la population collégienne est concernée par le phénomène, en tant qu'auteur, témoin ou victime.

Lire la synthèse : Un collégien sur cinq a été victime de « cyber-violence »
http://campus.lemonde.fr/campus/article/2014/11/27/un-collegien-sur-cinq-a-ete-victime-de-cyber-violence_4530528_4401467.html

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

Source et la suite sur :
http://campus.lemonde.fr/campus/article/2014/12/02/comment-combattre-la-cyber-violence-a-l-ecole_4532343_4401467.html

Cybercriminalité : le jeu en vaut-il la chandelle ?

Crédit Photo : Shutterstock

Cybercriminalité : le jeu en vaut-il la chandelle ?

Faire réaliser une page web factice pour faire du hammeçonnage ne coûte que 150 dollars

Attention, il n'est pas là question de dire qu'être un cybercriminel c'est bien… comme toute activité criminelle elle est punie par la loi avec des amendes et des peines de prison, nous y reviendront. Mais, tout de même, selon une étude Kaspersky, il semblerait que le ratio investissement/gains soit plus qu'intéressant… ce qui explique l'augmentation exponentielle de ce nouveau type de criminalité 2.0 qui ne nécessite plus du tout de courage. Assis tranquillement devant un ordinateur, les criminels n'ont plus rien à voir avec les gangsters des années 30.

Mais avant tout, une petite précision : tous les cybercriminels ne sont pas des hackers… et tous les hackers ne sont pas des cybercriminels. Bon nombre de cybercriminels ne font qu'acheter des logiciels préconçus par des hackers, les « Black Hats »… et il y a des hackers, les « White Hats », qui luttent justement contre ce derniers.

Le vol de données : peu d'investissement pour beaucoup de gain
Les cybercriminels qui ne veulent pas investir beaucoup dans un logiciel malveillant peuvent tout simplement faire du phising (hammeçonnage) de données. Pour 150 dollars, selon Kaspersky Lab, il est possible de se faire créer une page web similaire à celle visée (réseau social, site institutionnel, société…), de l'héberger et d'envoyer des spams (du style « Insérez vos données pour qu'on vous rembourse 450 euros de trop payé sur vos factures » et autres…)

Ce type de campagne de phising est souvent facilement décelable puisque de grossières fautes de grammaire et d'orthographe se glissent dans le texte. Mais malgré tout ça peut rapporter gros : en revendant les données ainsi captées (ne serait-ce que nom, prénom et adresse), le pirate peut toucher 100 dollars par personne touchée… avec 100 personnes touchées, les gains montent en flèche : 10 000 dollars.

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

Source : http://www.economiematin.fr/news-cout-cybrecriminalite-enjeu-gain-piratage-revente-donnees

---

Gmail et Inbox : Google va-t-il trop loin ?

Gmail et Inbox : Google va-t-il trop loin ?

Google vient de lancer Inbox, une version nouvelle et plus structurée de Gmail. La solution soulève de nombreuses questions autour de l'utilisation et de la protection des données personnelles et notamment : quel est l'objectif de Google avec Inbox ?

Inbox présente un grand nombre de fonctionnalités intéressantes : une bonne classification des e-mails, un algorithme intelligent, une interface plus ergonomique et facile à utiliser, en particulier à partir d'un téléphone mobile. Cependant, il subsiste quelques zones d'ombre, que ce soit avec Gmail ou Inbox.
Google se positionne parmi les acteurs qui protègent la vie privée de ses utilisateurs, alors qu'il met tout en œuvre dans ses outils pour analyser leur comportement. Nous savons tous que les données qui transitent dans nos e-mails sont analysées et utilisées, soit pour classer nos e-mails, soit pour nous envoyer/identifier une publicité ciblée. Google analyse les données et doit donc les stocker pour y avoir accès à tout moment.

Peut-on continuer à parler de vie privée lorsqu'il n'y a ni option ni moyen d'interdire l'accès à mes données ?
Inbox propose à l'utilisateur de faire le tri et de filtrer les e-mails commerciaux et les newsletters, que celui-ci peut désormais recevoir dans des catégories (« promotions », « réseaux sociaux », etc.). Pourtant, Google pousse des publicités vers les utilisateurs grâce à ce même outil. Alors Google est-il vraiment impartial lorsque Inbox filtre et classifie les e-mails ? La publicité est tout de même l'un des principaux revenus de Google… AdWords a d'ailleurs évolué pour devenir la principale source de revenus de Google et les recettes publicitaires totales de Google ont dépassées les 50 milliards de dollars en 2013, faisant de lui le leader, bien loin devant ses concurrents.
La principale différence entre Google Inbox et Gmail résulte dans l'affichage des publicités : apparemment, il n'y a pas de pub dans Inbox alors qu'il y en a toujours dans Gmail. Cela signifie-t-il que les publicités sont cachées… peut-être dans ce que Google appelle les « Bundle » (groupement de plusieurs emails) ? Car, il est difficile de croire que Google va supprimer l'affichage des publicités dans l'un de ses principaux services. Par contre, il est fort probable qu'ils continuent à utiliser l'une de leurs tactiques bien rodées qui consiste à promouvoir de nouvelles offres sans publicité au départ…
Avec Inbox, Google offre un algorithme, une classification et de nombreuses autres fonctionnalités d'un très bon niveau. Toutefois, sur le marché du filtrage des e-mails (de l'anti-spam à la solution de graymail management), seul Google a besoin de lire le contenu des e-mails alors que les autres acteurs se basent sur sa structure et d'autres paramètres pour définir sa nature. Par ailleurs, les pure-players qui offrent des solutions identiques de filtrage des e-mails, ne tirent aucun bénéfice de la publicité. Ils sont donc impartiaux dans la classification, aucun émetteur ne sera mis en avant au détriment d'un autre. Ainsi, le contenu des e-mails n'influence pas les contenus et les publicités lors des connexions du navigateur. On peut facilement comparer cette situation avec une affaire du passé concernant le paiement de Google vers AdBlock.
Les débats autour de la protection de la vie privée et des données personnelles n'ont jamais été aussi présents. Les solutions du type Gmail et Inbox sont largement utilisées par le grand public parce qu'elles sont gratuites et performantes. Toutefois, les utilisateurs n'ont pas forcément pris conscience de l'utilisation de leurs données. Quand une solution est gratuite, cela signifie que l'utilisateur est le produit… Si cela peut être acceptable pour le grand public (à voir sur le long terme), dans le monde de l'entreprise, la confidentialité des données doit être prise au sérieux. Le choix d'une solution de graymail management doit se faire en connaissance de cause.

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

Source : http://www.journaldunet.com/ebusiness/expert/59293/gmail-et-inbox–google-va-t-il-trop-loin.shtml

Données personnelles L’Europe prépare sa loi anti-Gafa

Données personnelles L’Europe prépare sa loi anti-Gafa

La bataille est relancée entre l'Europe et les géants américains de la Toile. Après la résolution symbolique adoptée par les députés européens pour le démantèlement des activités de Google, Paris et Berlin s'attaquent désormais au référencement payant au sein des moteurs de recherche. Les deux capitales ont adressé un texte à Bruxelles dans lequel ils réclament la création d'une loi pour imposer une plus grande transparence dans l'accès aux sites internet de Facebook, Google, Amazon et Apple, surnommés «GAFA».

Les deux capitales réclament un «traitement transparent et non discriminatoire» des sites. La nouvelle loi, qui sera tout sauf symbolique, ciblera également Facebook qui vient de modifier ses conditions d'utilisation en élargissant l'usage de données personnelles des utilisateurs pour mieux cibler les publicités.
Elle veut rendre le contrôle sur leur vie digitale et leurs données aux utilisateurs et leur redonner la liberté de choix pour l'utilisation d'applications ou de services sur ces plates-formes. Dans un texte adressé à la Commission européenne, les deux capitales, sans jamais citer le nom des sociétés mises en cause, désignées comme les «plates-formes indispensables» de l'Internet, réclament un «traitement transparent et non discriminatoire» des sites. Et ce en référence aux accusations de pratiques anti-concurrentielles dont Google fait l'objet de la part des deux pays. Ainsi, les deux États demandent à Bruxelles de lancer, dès l'année prochaine une consultation publique. Une mesure que la Commission européenne se dite prête à prendre.
Parallèlement, les établissements européens de protection des données personnelles passent eux aussi à la charge. Ils ont publié un ensemble de règles encadrant le droit à l'oubli. Parmi leurs doléances, le groupement réclame l'extension du droit à l'oubli à tous les noms de domaine, y compris en «.com». Le droit à l'oubli ne doit plus seulement concerner les déclinaisons nationales de Google, mais l'universaliser.

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

Source : http://www.leconomiste.com/article/962737-donnees-personnellesl-europe-prepare-sa-loi-anti-gafa
par M. L.

Piratage de Sony Pictures : le FBI met en garde contre un malware « destructeur »

Piratage de Sony Pictures : le FBI met en garde contre un malware « destructeur »

Le piratage massif de Sony Pictures Entertainment la semaine dernière a motivé le FBI à tirer la sonnette d'alarme. Le bureau fédéral, qui enquête sur l'affaire, met en garde les entreprises concernant un logiciel malveillant « destructeur » utilisé par les pirates.

De toute évidence, le FBI ne prend pas le piratage de Sony Pictures à la légère. Le bureau fédéral d'investigation a communiqué par voie de presse pour mettre en garde les entreprises contre un nouveau malware. Ce dernier est décrit comme étant « destructeur », et serait à l'origine des déboires de Sony, dont plusieurs films encore inédits aux Etats-Unis ont été mis en ligne dans des versions piratées. Il faut cependant préciser que, dans son rapport d'alerte, le FBI ne cite jamais le nom de Sony. Néanmoins, pour des experts en sécurité interrogés par l'agence Reuters, il ne fait aucun doute que les autorités évoquent bien cette affaire.
Selon le FBI, « il s'agit de la première cyber-attaque destructrice menée contre une entreprise sur le sol américain ». Des manœuvres similaires ont été constatées en Asie et au Moyen-Orient, mais jamais aux USA jusqu'à aujourd'hui.

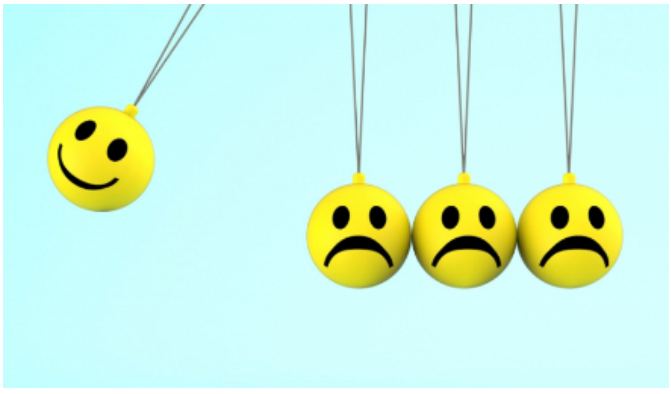
Concrètement, le logiciel malveillant remplace petit à petit les données présentes sur le disque dur, y compris dans les secteurs d'amorçages qui permettent à l'ordinateur de démarrer. Le système se retrouve donc bloqué, à la merci des pirates qui contrôlent le malware.
« Le FBI conseille régulièrement le secteur privé de divers indicateurs de cyber-menaces observés au cours de ses enquêtes » explique le porte-parole du bureau, Joshua Campbell. « Ces données sont fournies afin d'aider les administrateurs systèmes à se protéger des actions permanentes des cyber-criminels. » Les entreprises victimes de ce type d'attaques sont invitées à contacter les autorités au plus vite.

Du côté de Sony, si un porte-parole a récemment déclaré que l'entreprise avait d'ores et déjà restauré « un certain nombre de services importants », de nombreux documents ont été récupérés par les pirates durant l'intrusion, et pas seulement des films du studio. Des contrats de tournage et des papiers d'identité de certains comédiens font partie des fichiers volés. Quant à l'origine de l'attaque, elle reste toujours à confirmer, même si les soupçons sont tournés vers la Corée du Nord, qui n'aurait pas apprécié la sortie du film « L'Interview qui tue », comédie qui prend pour cible le régime politique du pays.

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

Source : http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-742501-piratage-sony-fbi-garde-malware-destructeur.html?estat_svc=s%3D223023201608%26crmID%3D639453874_766966538

Détecter et analyser les émotions sur internet



Détecter et analyser les émotions sur internet

Détecter et analyser les émotions humaines au départ de sites internet, c'est ce que propose Getsmily, une nouvelle spin-off de l'Université catholique de Louvain. « Avec plus d'un milliard de sites web sur la toile, le besoin pour les entreprises de nouer des liens forts avec leurs publics devient primordial. Et La construction de ces liens commence par la compréhension des comportements et des émotions de ces audiences. Les émotions nous animent au quotidien et guident nos actions, plus souvent qu'on ne le pense », confie David Frenay, le chercheur UCL à la base de la technologie et CTO de la startup.

Fruit de plusieurs années de travail au sein du laboratoire de vision par ordinateur du professeur Benoit Macq de l'UCL, cette technologie a séduit des investisseurs privés ainsi que le Fonds d'investissement VIVES II qui ont décidé d'injecter un demi-million d'euros dans la société. Les applications marketing rendues possibles grâce à la technologie UCL, unique en son genre, vont mener l'équipe de GetSmily à la conquête du world wide web. « La compréhension des émotions humaines et les leviers qui les activent sont des atouts majeurs pour le responsable marketing moderne. Le marketing reprend donc un rôle central au sein des entreprises qui sont résolument tournées vers l'avenir », confirme David Hachez, co-fondateur et CEO de GetSmily.
Lancée en septembre 2014, la spin-off GetSmily donne accès à un indicateur de performance émotionnelle novateur baptisé l'Emoscore. Celui-ci est obtenu grâce aux Emolytics (contraction des mots « emotions » et « analytics ») qui intègrent un algorithme unique et scientifiquement solide. La technologie a déjà séduit plusieurs entreprises telles que Foto.com, Europ Assistance, VOO, La Loterie Nationale, Sherpa, Quick Step, Lampiris ou encore Rossel Advertising.
GetSmily résulte d'un projet de recherche dans le domaine de la vision par ordinateur (vision artificielle), accompagné pendant deux ans par le Louvain Technology Transfer Office (LTTO). « Cette nouvelle spin-off démontre le rôle important que joue le LTTO pour assurer avec succès le transfert de technologie issu de la recherche UCL. Le soutien de la région wallonne (DG06), notamment par le biais de son programme First Spin-Off et du fonds proof-Of-Concept nous a permis de concrétiser ce projet qui offre de belles perspectives de développement », déclare Anne Bovy, co-directrice du LTTO et directrice de l'administration de la recherche de l'UCL. Les investisseurs qui rejoignent GetSmily vont lui permettre d'accélérer son développement international et aideront l'équipe à résoudre les challenges techniques qui s'annoncent. « Investir dans une startup du web confirme la volonté de notre fonds d'être un acteur dans ce secteur en pleine ébullition tout en soutenant le développement d'une spin-off de l'UCL », souligne Philippe Durieux, CEO de VIVES II.

A propos de GetSmily
Les Emolytics de GetSmily permettent aux propriétaires de sites internet de mesurer les émotions de leur audience ainsi que leurs comportements de surf. GetSmily, qui compte déjà 5 personnes à son bord, propose son produit Emolytics en 14 langues en mode SaaS (Software as a service) avec les plans Free, Start, Pro et Enterprise. Les données statistiques anonymes collectées sont traitées pour prendre forme dans un rapport. Ce dernier guide les entreprises dans la mesure de la qualité de la relation avec leurs audiences/publics, par l'intermédiaire d'un KPI unique appelé Emoscore, ainsi qu'à la prise de décision stratégique (marketing, communication, technique et/ou managériale).

Les fondateurs :
– David Hachez, CEO de GetSmily. Il a déjà à son actif quelques initiatives dont Raz*War, lancé en 2009 et repris par un fonds d'investissement privé en 2012
– David Frenay, ingénieur civil biomédical, master en physique et en gestion à l'UCL, bachelier en mathématique et médaillé aux Olympiades internationales. Il est à l'origine de la technologie de détection des émotions et occupe aujourd'hui le poste de CTO

A propos de VIVES – Louvain Technology Fund et du LTTO
– VIVES – Louvain Technology Fund est un fonds d'investissement technologique multi-sectoriel qui investit dans les spin-offs de l'UCL et dans les start-up en Belgique et dans les pays limitrophes. L'objectif du fonds est d'investir dans le développement de start-up, depuis la validation technologique jusqu'à la maturité commerciale. Les fonds (VIVES 1 de 15 millions d'euros et VIVES 2 de 43 millions d'euros) sont gérés par la Sopartec, la société de transfert de technologie de l'UCL. Infos : http://www.vivesfund.com.

– Le Louvain Technology Transfer Office (LTTO), regroupant la Sopartec et l'administration de la recherche de l'UCL, couvre l'entièreté du processus de transfert de technologie : financement des contrats de recherche, identification des inventions dans les laboratoires, protection et gestion de la propriété intellectuelle, maturation technologique et commercialisation (par le biais de licences et/ou spin-off). Plus précisément, la Sopartec coordonne la gestion des accords de licence et la maturation technologique des projets de spin-offs de l'UCL. Plus de 60 spin-offs, qui génèrent aujourd'hui, plus de 3.000 emplois, ont été créées en se basant en tout ou en partie sur des résultats des recherches menées à l'UCL. Il s'agit notamment de Ion Beam Application (IBA), IRIS Groupe, IBT, Telemis, Viridaxis, Promethera, GreenWatt, Keemotion, Iteos Therapeutics, DelfMens, Novadip Biosciences, etc. Infos : http://www.ltto.com.

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

Source : http://www.bulletins-electroniques.com/actualites/77248.htm

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: Bing s’y met aussi

Droit à l’oubli: Bing s’y met aussi

Après Google, Bing vient de mettre à disposition des internautes européens un formulaire en ligne qui leur permet de demander le retrait d’informations les concernant.

Bing a commencé à supprimer la liste des résultats de recherche des internautes européens ayant invoqué leur droit à l’oubli, a indiqué le service de suppression des requêtes Forget.me.

Suite à une décision de la Cour de justice de l’Union européenne rendue en mai dernier, le moteur de recherche de Microsoft a démarré ces suppressions en juillet en publiant un formulaire que les utilisateurs doivent remplir. Forget.me précise que ceux qui ont demandé à Bing de supprimer les résultats de leurs requêtes ont commencé à recevoir des réponses. 699 demandes de désindexation sur Bing ont été réalisées via Forget.me depuis le 23 juillet, ce qui représente 2 362 URLs. A ce jour, 79 demandes ont fait l’objet d’une réponse de Bing.
Bing représente 22% des demandes envoyées via Forget.me depuis le 23 juillet, 78% des demandes étant destinées à Google. En moyenne les utilisateurs soumettent moins d’URL par demande à Bing qu’a Google : 3,4 pour Bing contre 9,1 pour Google.
Accédez au formulaire de déférencement de Google

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

Source : http://www.lemondeinformatique.fr/actualites/lire-droit-a-l-oubli-bing-s-y-met-aussi-59438.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

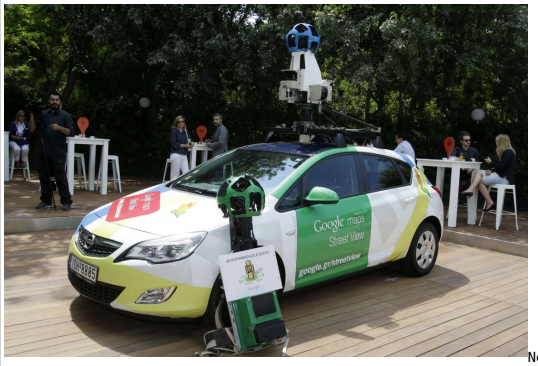
---

Vous avez peur de Facebook ? Méfiez-vous plutôt de… tout

Vous avez peur de Facebook ? Méfiez-vous plutôt de… tout

« En réponse aux nouvelles lignes directrices de Facebook et en vertu du code de la propriété intellectuelle, je déclare que mes droits sont attachés à toutes mes données personnelles, dessins, peintures, photos, textes, musiques… publiés sur mon profil. Pour une utilisation commerciale, mon consentement écrit est nécessaire. »

Le message s'est répandu comme une traînée de poudre sur le réseau social, depuis l'arrivée d'une nouvelle politique de confidentialité. 240 mots qui seraient censés mettre à l'abri l'internaute contre une éventuelle réutilisation de ses données personnelles, mais qui n'ont « aucune valeur juridique », pointe la Commission nationale de l'informatique et des libertés (Cnil).
Pour autant, ce message (qui a déjà sévi en 2012) révèle un malaise des Français face à Facebook. Comme après le (faux) bug qui a suscité une panique sur le réseau social, les internautes ne sont pas à l'aise avec l'utilisation de leurs données personnelles.
Un sondage BVA, diffusé par « 20 minutes », pointe ainsi que 58% des Français ont une mauvaise opinion de Facebook. Celui qui compte 28 millions d'utilisateurs dans l'Hexagone voit son image bien plus écornée qu'Amazon ou Apple. Pis, Google s'en tire avec une perception « plutôt bonne » auprès de 81% des sondés. Erwan Lestrohan, directeur d'études de BVA Opinion, explique au quotidien :
Sur Google, on entre des mots-clés. Sur Apple et Amazon, des données bancaires. Facebook est la seule [plateforme] sur laquelle on stocke de nombreuses données privées. Ça génère un peu plus d'inquiétudes et ça touche plus à l'affect. »



Ne pas oublier le (condamné) Google

Cette crainte réelle se justifie en partie. Dans ses conditions d'utilisation, le réseau social prévoit que l'internaute lui « donne l'autorisation d'utiliser » les informations personnelles, dont les photos, qui sont partagées sur la plateforme.
Néanmoins, il faut reconnaître que Facebook a fait de nombreux efforts pédagogiques pour expliquer ses pratiques et surtout permettre aux utilisateurs de mieux se saisir des paramètres de confidentialité. Ainsi, la nouvelle politique d'utilisation des données s'est accompagnée d'une page – intitulée « Vous avez le contrôle » – permettant de mieux comprendre et appréhender les retords paramètres. En somme, une sorte de tutoriel géant sur l'utilisation avancée de Facebook.

Evidemment, il convient de prendre au sérieux les empiètements sur la vie privée sur internet. Seulement, Facebook est loin d'être le seul acteur qui doit préoccuper les internautes. Google devrait même arriver en tête de ce classement.

L'Américain est en effet en capacité de dresser un incroyable profil des consommateurs en se basant sur son énorme base de données personnelles. D'abord, il dispose d'un historique de l'ensemble des recherches effectuées sur le web, mais aussi ses robots lisent les contenus des e-mails, tandis que les smartphones Android enregistrent les géolocalisations tout en comptant le nombre de pas… A ces couches pourraient bientôt s'ajouter les équipements Nest, permettant d'en savoir plus sur les pratiques dans la maison.
Effrayant ? C'est peu de le dire. Surtout que l'intégralité de ces informations sont croisées. C'est d'ailleurs pour cette raison que la Cnil a condamné le géant à 150.000 euros d'amende (soit 0.01% de ses recettes annuelles dans l'Hexagone).
L'ensemble de ces données sont utilisées afin de prédire ce que le consommateur va chercher, lire, acheter, faire…

Cinq ans et aucune avancée…
Google, Amazon ou Apple ne sont pas les seuls acteurs dont il convient de se méfier. Un large écosystème d'entreprises s'est créé avec pour seul objectif de traquer le comportement de l'internaute. Un graphique de la société de conseils Luma Partners met ainsi en lumière qu'un nombre impressionnant de sociétés se greffe à un contenu.

La Cnil a ainsi mis à disposition un outil de visualisation (http://www.cnil.fr/vos-droits/vos-traces/les-cookies/telechargez-cookieviz/) de l'impact d'une navigation internet, et de l'ensemble des acteurs qui entrent en jeu. De son côté, le Massachusetts Institute of Technology (MIT) propose un service (https://immersion.media.mit.edu) qui, à partir d'une adresse e-mail Gmail, Yahoo ou Microsoft, permet de déceler les liens entre personnes, ainsi que leur importance.
Dans l'idéal, il faudrait que l'internaute donne un accord manifeste à chaque site qui veut utiliser ses données personnelles », estime Olivier Cimelière, président du cabinet en communication Heuristik. « Mais plutôt que ce contrat moral, dit d'opt-in, c'est la politique d'opt-out qui prévaut sur les sites, c'est-à-dire que l'option est activée par défaut et que la désactiver est compliqué et fastidieux. »

Un avis de la Commission nationale de l'informatique et des libertés (Cnil) de 2009 demandait déjà aux fournisseurs de réseaux publicitaires d'adopter au plus tôt des mécanismes d'opt-in pour informer au préalable la pub ciblée. Cinq ans plus tard, la pratique ne semble pas appliquée par les géants, malgré un relais de l'avis auprès du G29 européen.

« La norme sociale a évolué »
Faut-il baisser les bras face aux pratiques des acteurs du net qui empiètent sur la vie privée ? « La vie privée peut être considérée comme une anomalie », a lâché Vinton Cerf, père fondateur du web devenu « chef évangéliste » chez Google, rejoignant les saillies régulières de Mark Zuckerberg, PDG et cofondateur de Facebook. « Les gens sont désormais à l'aise avec l'idée de partager plus d'informations différentes, de manière plus ouverte et avec plus d'internautes. […] La norme sociale a évolué », a-t-il notamment estimé.

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

Source et suite : http://obsession.nouvelobs.com/high-tech/20141201.OBS6646/vous-avez-peur-de-facebook-mefiez-vous-plutot-de-tout.html