

Que sont prêts à accepter les Français de leurs données personnelles ?



Que sont
prêts à
accepter les
Français de
leurs
données
personnelles
?

Havas Media Group France vient de publier les résultats d'une étude qui dresse l'état des lieux du rapport entre les Français et la Data. Des Français conscients et inquiets mais qui n'hésitent pas à donner leur données ; à condition d'obtenir des contreparties.

Des Français inquiets...

Havas Media a interrogé 1000 internautes représentatifs de la population française, âgés de 15 à 64 ans. Le premier enseignement est qu'ils sont parfaitement conscients de la transmission de leurs données à des tiers. 93% savent qu'elles sont captées et 84% s'en inquiètent. Trois craintes se dégagent : 74% des internautes ont peur de l'usage frauduleux des données, 53% ont peur que des détails de leur vie intime soient révélés et 47% craignent la surveillance des autorités.

... mais opportunistes

Cependant, 46% des Français voient cette utilisation de leurs données comme une opportunité. 45% sont prêts à laisser les entreprises suivre leurs données, moyennant une contrepartie financière. Près de 42% des internautes interrogés sont prêts à l'accepter contre une contrepartie non-financière.

La typologie des Français vis-à-vis de leurs données personnelles

Grâce aux réponses fournies par l'échantillon interrogé, Havas Media a pu segmenter les internautes en cinq profils distincts. Chaque groupe a des comportements et des attentes spécifiques.

Data Natives – 24%. Une population plutôt jeune (15 à 25 ans), consciente de la captation des données personnelles mais peu inquiète. Pour eux, c'est normal, habituel, ils ne se protègent ni plus ni moins que les autres et n'attendent pas grand chose de la transmission des données.

Data Stratèges – 9%. Ils sont plus âgés (35 à 49 ans) et tout à fait conscients. Ils font plus attention aux données qu'ils fournissent et cherchent à obtenir des contreparties.

Data Fatalistes – 27%. Cette population est assez jeune, consciente, inquiète mais fataliste. Ils savent que leurs données sont captées mais ne maîtrisent pas vraiment la confidentialité de leurs données. Ils se protègent peu, par négligence.

Data Parano – 36%. Ils sont plus âgés, conscients et très inquiets. Ils ne voient aucun intérêt dans la captation de leurs données personnelles. Ils craignent tout : l'utilisation frauduleuse de leurs données, la surveillance généralisée et la diffusion de données privées. Ils ne comprennent pas tout mais cherchent à se protéger du mieux qu'ils peuvent.

Data Détendus – 4%. Cette population est indifférente au phénomène. Ces internautes sont peu conscients et donc peu inquiets. Ils pensent pouvoir tirer un bénéfice de la captation de leurs données mais restent passifs et fournissent de nombreuses données personnelles.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

<http://www.blogdumoderateur.com/etude-havas-media-francais-donnees-personnelles/>

JP Morgan piraté : les données de 83 millions de clients exposées



JP Morgan, piraté :
les données de 83
millions de
clients exposées

Cet été, JP Morgan a été victime d'une attaque informatique de grande envergure. La banque américaine admet que les données de 83 millions de clients ont pu être exposées. Toutefois, il ne s'agirait pas d'informations sensibles pour la porte-parole de la société.

76 millions de foyers et 7 millions de PME seraient concernés par ce qui pourrait être l'une des plus grandes fuites de données de l'histoire. Cet été, les systèmes informatiques de la banque JP Morgan ont été compromis par une attaque ayant permis aux pirates d'accéder aux noms, adresses, numéros de téléphone, et adresses e-mail de 83 millions de clients, annonce JP Morgan dans un document transmis à la SEC, le gendarme américain de la bourse.

La banque ajoute qu'il n'y a « pas de preuve » que des données sensibles comme les numéros de comptes, mots de passe, identifiants, dates de naissance ou numéros de sécurité sociale aient été compromises. Les responsables de l'attaque n'auraient pas eu accès à ce type de données sensibles, pense Patricia Wexler, porte-parole de JP Morgan. Il ne serait donc pas nécessaire que les clients changent leurs mots de passe.

Pour le moment, la banque n'aurait pas constaté de fraude relative à cet incident.

Mais l'attaque, très sophistiquée, aurait tout de même permis aux pirates d'accéder « au plus haut niveau des droits administrateurs » selon le New York Times qui s'appuie sur des sources proches du dossier. Puis, les informations exposées restent potentiellement utiles aux cyber criminels : « ils pourraient littéralement utiliser l'identité de ces 83 millions de personnes et entreprises », affirme Tal Klein, de la société de sécurité informatique Adallom, à l'agence Reuters.

La banque avait annoncé en août qu'elle enquêtait avec les autorités sur une attaque informatique. Le FBI soupçonnait des pirates russes en raison de la crise ukrainienne et des sanctions économiques à l'encontre du régime de Moscou. Le New York Times affirmait que JP Morgan n'était pas la seule banque concernée mais qu'en tout, cinq banques auraient été visées le même mois.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

<http://pro.clubic.com/it-business/securite-et-donnees/actualite-730905-clients-jp-morgan-pirates.html>

Cookies : ça y est, la Cnil commence à contrôler les sites français



Cookies : ça
y est, la
Cnil
commence à
contrôler
les sites
français

Les contrôles de la Cnil commencent. La Commission va vérifier que les sites Internet français utilisant des cookies publicitaires ou de mesure d'audience invitent les visiteurs à leur consentement préalable.

« En utilisant ce site, vous acceptez l'utilisation de cookies permettant de vous proposer des contenus et des services adaptés à vos centres d'intérêts. » Le message a fleuri le Web français depuis décembre 2013. Il est la conséquence directe d'une recommandation de la Cnil découlant d'une directive européenne de 2011.

Celle-ci explique que « les traceurs (cookies ou autres) nécessitant un recueil du consentement ne peuvent (pas) être déposés ou lus sur son terminal, tant que la personne n'a pas donné son consentement ».

A partir de ce mois d'octobre, la Commission va procéder à des contrôles. Tout acteur contrevenant à cette obligation s'expose à une amende pouvant atteindre 150 000 euros. Voici un rappel pour être conforme :

Mettre son site Web en conformité. Qui est concerné par cette obligation ?

Les responsables de sites, éditeurs d'applications mobiles, régies publicitaires, réseaux sociaux et éditeurs de solutions de mesure d'audience.

Quels sont les cookies concernés par la loi ?

Les cookies liés aux opérations publicitaires, comme le traçage comportemental, les cookies des réseaux sociaux générés par les boutons de partage ainsi que certains cookies de mesure d'audience.

Quelles sont les obligations légales ?

Informers les internautes de la finalité des cookies, obtenir leur consentement et leur fournir un moyen de les refuser. A noter que la durée de validité de ce consentement est de 13 mois maximum.

Quels sont les cookies exemptés ?

Les cookies utilisés pour un panier d'achat de site marchand, l'identification pour la durée d'une session, l'authentification, la lecture de fichiers multimédias, l'équilibrage de charge, l'analyse d'audience (dans certains cas) ou encore la personnalisation de l'interface utilisateur.

Consciente que la mise en conformité avec ces dispositions présente, selon les cas, une certaine complexité, la Cnil consacre désormais une partie de son site Web à ce sujet. Elle explique quelles sont les façons de mesurer l'audience afin d'être exempté du message de consentement préalable. La Commission explique aussi comment recueillir ce consentement pour les outils comme Google Analytics ou Universal Analytics. La Cnil dispose enfin de solutions pour les boutons de partage sociaux ou pour les sites multipliant les cookies.

Préparer un contrôle de la Cnil

Il faut tout d'abord savoir que la décision de procéder à une vérification est prise par le président de la Cnil, sur la proposition du service des contrôles. La décision de prévenir, ou non, le responsable du site Web qui va faire l'objet de cette visite est « prise en opportunité », ce qui signifie qu'elle ne sera pas systématique. La Cnil peut aussi exiger la fourniture de documents en amont de sa visite. Voici le déroulé d'un contrôle :

Une mission de contrôle vise prioritairement à obtenir copie du maximum d'informations, techniques et juridiques, pour apprécier les conditions dans lesquelles sont mis en œuvre des traitements informatiques. La délégation de la Cnil peut demander communication de tous documents nécessaires à l'accomplissement de sa mission, quel qu'en soit le support, et en prendre copie.

Les contrôleurs peuvent accéder aux programmes informatiques et aux données, et en demander la transcription pour les besoins du contrôle.

La délégation peut demander copie de : contrats (ex.: contrats de location de fichiers, contrats de sous-traitance informatique), formulaires, dossiers papiers, bases de données, etc.

Un procès-verbal de fin de mission est établi à l'issue du contrôle, pour préciser notamment la liste des documents dont une copie a été effectuée.

Cet article vous a plu ? Laissez-nous un commentaire (Source de progrès)

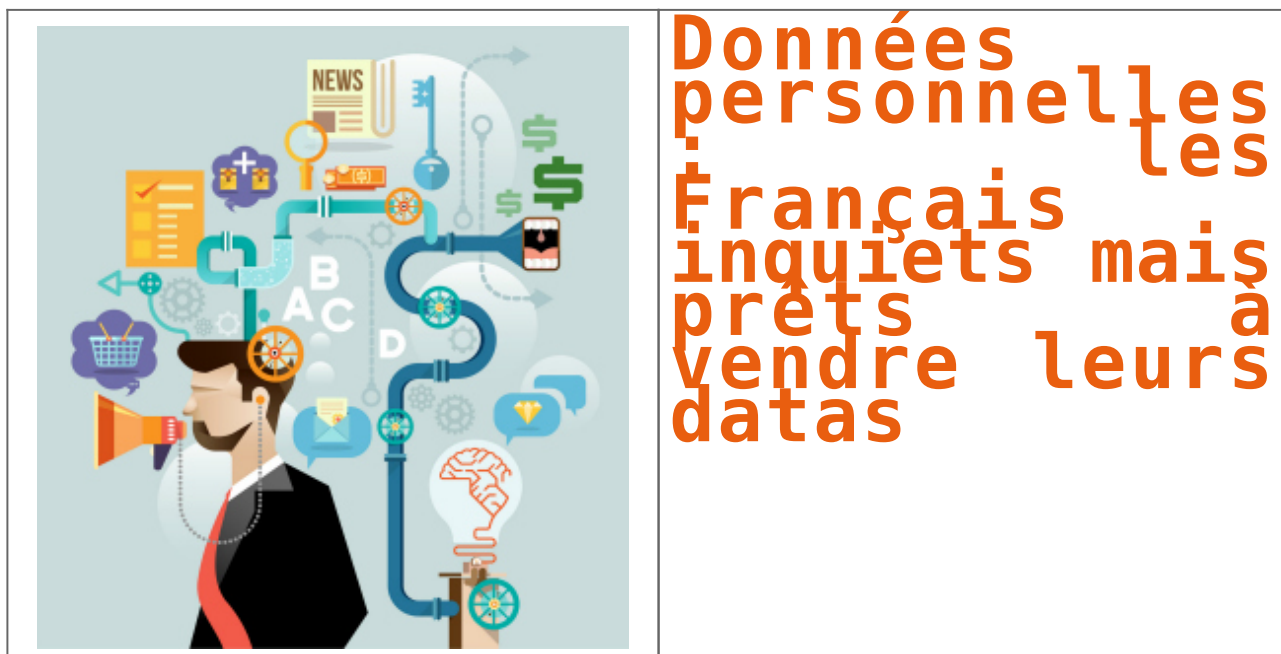
Source :

<http://pro.clubic.com/legislation-loi-internet/cnil/actualite-730529-cnil-controles-rappel-commerçants.html>

Information importante pour votre site Internet. Les grands changements de 2014

Traitements de données personnelles non déclarés à la CNIL, mentions légales absentes ou incomplètes, conditions générales non réglementaires... d'après le baromètre d'E-Mail Brokers, les mauvaises pratiques sont légion sur les sites professionnels français.

Données personnelles : les Français inquiets mais prêts à vendre leurs datas



Données
personnelles
les
Français
inquiets mais
prêts à
vendre leurs
datas

Le grand écart des internautes au sujet de l'exploitation de leurs données personnelles se poursuit. Si les Français sont conscients en très grande majorité de cette collecte, et même inquiets de ce qui en est fait, ils sont dans le même temps tout à fait prêt à les monnayer au plus offrant.

On n'est jamais mieux servi que par soi même... Telle pourrait être la conclusion de ce sondage mené par Toluna pour Havas Media auprès d'un échantillon de 1000 internautes français du 5 au 20 août. Etant donné que les géants du Web vendent des « profils » aux annonceurs ou aux géants du marketing, pourquoi ne pas en profiter directement ?

« Data fatalistes »

Ainsi, 45% des internautes interrogés sont prêts à partager leurs données moyennant des contreparties financières. 30% estiment que 500 euros seraient suffisant pour un partage intégral pendant un an, et 42% contre des contreparties non financières (gain de miles, réductions, cadeaux). Vous avez dit paradoxal ?

« C'est le nouveau paradoxe français, les internautes sont très conscients de la captation de leurs données, sont inquiets, mais ils ont un appétit de voir ce que cela peut créer pour eux », indique Raphaël de Andréis, directeur général Havas Media Group France, à l'AFP.

Cette tentation de monnayer ses datas ne s'applique évidemment pas à toutes les tranches d'âge. Les « plus de 35 ans », appelés « data paranos » sont les moins enclins à partager quoi que ce soit : « Ce sont les plus rétifs, qui ne vivent pas bien la captation de leurs données. Les marques et les médias doivent les rassurer sur l'usage qui peut être fait de leurs données », commente le PDG d'Havas Media France, Raphaël de Andreis. Les « data natives », âgés de 15 à 24 ans, sont au contraire les moins inquiets. Puis il y a les « data fatalistes », qui représentent les internautes ayant accepté que leurs informations privées soit divulguées et considèrent qu'ils ne peuvent rien y faire.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

<http://www.zdnet.fr/actualites/donnees-perso-les-francais-inquiets-mais-prets-a-vendre-leurs-datas-39806957.htm>

Le droit à l'oubli : une menace pour l'e-reputation ?



Comité consultatif de Google
sur le droit à l'oubli

Le droit à l'oubli : une menace pour l'e-reputation ?

Le 13 mai 2014, la Cour de justice de l'Union européenne rendait un arrêt instaurant la notion de droit à l'oubli sur les réseaux numériques. Les internautes ont désormais la possibilité de demander aux moteurs de recherche le retrait de certains contenus qui apparaissent dans la liste de résultats. Si c'est une vraie aubaine pour la gestion de l'e-réputation des particuliers, les professionnels ne sont pas logés à la même enseigne.

En France, le « droit à l'oubli » n'est pas nouveau. On trouve les premières traces de ce principe dans la Loi informatique et libertés de 1978. Celle-ci précise que des données personnelles peuvent être collectées lorsqu'elles « sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ».

Plus tard, en 2011, cette loi connaît une évolution fondamentale et étend le domaine de ce droit. Le texte ouvre ainsi à toute personne physique justifiant de son identité le droit d'exiger que soient « rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexacts, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ».

Alors que propose de nouveau l'arrêt de la CJUE du 13 mai 2014 ?

Une couverture élargie au niveau européen ? Oui, mais pas seulement. En fait, plutôt que de parler de droit à l'oubli, la notion de « droit au déréférencement » semble plus adéquate pour cet arrêt. Il n'est pas question de « supprimer » une information, mais de ne plus la référencer dans les moteurs de recherche. C'est justement le champ d'application de l'e-réputation : effacer les traces. Pour autant, ce nouvel arrêt aux contours très rigides a peu de chances de modifier la façon de travailler des professionnels de l'e-réputation.

Le cadre ne privilégie pas les professionnels

Si le cadre est plutôt rigide, la question de savoir si Google va accaparer une partie de l'activité des spécialistes de l'e-réputation pour des demandes de déréférencements simples (que ce soit pour les postes en interne dans les grands groupes, ou pour les prestataires de services spécialisés) se pose.

Dans le cadre actuel (qui est amené à évoluer), ce n'est pas encore le cas. Comme le souligne Raphaël Brun, spécialiste de la sécurité des données pour le cabinet de conseils Solucom « l'arrêt de la CJUE du 13 mai 2014 ne concerne ni les entreprises, ni les personnes morales, ni les personnes publiques ».

Pour autant, un chef d'entreprise peut faire une demande à titre personnel. Si elle a des chances de passer pour des structures de type TPE-PME, pour lesquelles il est souvent difficile de dissocier vie privée et vie professionnelle des dirigeants, il n'en va pas de même pour les grands comptes. De plus, un grand patron peut aussi être vu comme un personnage public, ce qui rendra une demande de déréférencement encore plus difficile.

Dans ce cas, les professionnels devront continuer de travailler de manière classique : avec des prestataires spécialisés dans la gestion de l'e-réputation, comme Reputation Squad ou Reputation VIP par exemple, qui ne voient pas dans le formulaire de Google, ni dans l'arrêt de la CJUE, une nouvelle forme de concurrence (pour l'instant).



Droit à l'information contre droit à l'oubli

Pour rappel, l'arrêt de la CJUE du 13 mai 2014 vise tous les moteurs de recherche. Et en premier lieu Google, qui accapare la grosse majorité des recherches en Europe de l'Ouest et en Amérique du Nord. Et c'est justement Google qui, en premier, a mis en œuvre un formulaire pour se mettre en conformité. Google permet toutefois de distinguer un élément important : la dualité entre le droit au respect de la vie privée d'un côté, et le droit à l'information de l'autre. Un difficile équilibre à trouver pour les spécialistes de l'e-réputation. Car le droit à la liberté d'expression est lui aussi très encadré.

L'article 10 de la Convention européenne des droits de l'homme l'affirme clairement : « Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière ». En France, le Tribunal de Grande Instance (TGI) décidait en 2009 que « le principe constitutionnellement et conventionnellement garanti de la liberté d'expression interdit de retenir une atteinte distincte liée à une éventuelle violation des règles instituées par la loi du 6 janvier 1978 » (informatique et libertés, qui garantit l'encadrement de l'utilisation des données informatiques).

Une demande de déréférencement adressée à un moteur de recherche doit donc être très bien motivée, sachant que ce n'est pas un tribunal qui statue (du moins en premier lieu), mais une société privée, nord-américaine de surcroît (Google, Microsoft pour Bing, Yahoo...), pour qui le droit d'expression est extrêmement fort. « Le droit à l'oubli est désormais reconnu, mais il s'agit d'un droit pondéré, pas systématique. Il faut qu'il y ait matière à modifier ou effacer des données » précise Maître Gérard Haas, avocat à la cour d'appel de Paris, spécialiste du droit de l'Internet.

C'est un élément qu'il faut impérativement prendre en compte, car Google, par exemple, ne fait qu'un traitement par URL. Ce qui veut dire que son avis est définitif. Le cadre de l'arrêt est donc plus rigide que la marge de manœuvre proposée par les agences d'e-réputation.

Une faille à l'international

D'autres défauts viennent rendre moins efficace la tâche de Google, Microsoft et Yahoo. Si pour un particulier, un simple déréférencement en France peut suffire dans la plupart des cas, il n'en va pas de même pour un professionnel, à plus forte raison pour une multinationale : pas de gestion de l'e-réputation efficace sans déréférencement mondial. Pourtant, l'application de l'arrêt de la CJUE s'arrête à ses frontières.

Un lien déréférencé en France (Google.fr), ne le sera pas aux États Unis par exemple, ou sur une version internationale, en .com. « L'information reste accessible à partir du moment où une recherche se fait sur un nom de domaine hors Union européenne » précise Raphaël Brun de Solucom « A mon sens, c'est contraire à la loi, et contraire au futur règlement Européen. Quand une loi vise un citoyen Européen, elle est applicable partout dans le monde. On ne devrait pas retrouver une information le concernant sur Google.com. Je suis surpris que l'Union Européenne ne semble pas vouloir faire évoluer Google sur ce point ».

Dans ce contexte, l'arrêt de la CJUE n'intéressera pas une entreprise qui s'ouvre à l'international, ou une multinationale, dans sa gestion de l'e-réputation.

La décision de l'Europe comporte également un autre défaut majeur, l'effet Streisand pourrait bien s'appliquer en l'espèce. Bien connu des spécialistes de l'e-réputation, l'effet Streisand « est un phénomène médiatique au cours duquel la volonté d'empêcher la divulgation d'informations que l'on aimerait garder cachées, qu'il s'agisse de simples rumeurs ou de faits vérifiés, déclenche le résultat inverse. Par ses efforts, la victime encourage malgré elle l'exposition d'une publication qu'elle souhaitait voir ignorée ».

C'est justement le cas avec l'Espagnol Mario Costeja Gonzales, qui suite à une demande de déréférencement auprès de l'AEPD (l'équivalent de la CNIL espagnole), a déclenché une affaire avec Google qui a mené la CJUE à rendre l'arrêt du 13 mai 2014... et donc à sur-médiatiser son cas.

De plus, les liens déréférencés par Google sont « re »référencés par des sites hors Union Européenne, comme sur le site hiddenfromgoogle par exemple. Dans des cas sensibles de problématiques d'e-réputations, une requête « au grand jour » auprès d'un moteur de recherche (qui indique pourquoi un déréférencement a eu lieu) pourrait mettre en lumière l'affaire, et diriger les curieux vers ces sites de « re »référencements : un parfait cas d'effet Streisand.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

http://pro.clubic.com/webmarketing/referencement-naturel/article-729049-1-droit-oubli-change-reputation.html?estat_svc=s%3D223023201608%26crmID%3D639453874_679296180

Le droit à l'oubli comment ça marche ?



Le droit à l'oubli comment ça marche ?

Suite à la mise en place du Droit à l'oubli Internet, nous vous proposons de revenir sur les points essentiels de cette mesure. Grâce à l'infographie ci-dessous, vous pourrez vérifier si vous êtes éligible à une demande de désindexation de résultats, consulter les étapes nécessaires pour soumettre votre demande ou encore connaître les recours qui existent si votre démarche n'aboutissait pas.

Droit à l'oubli mais pas droit à l'erreur

Prenez bien soin de rédiger votre demande correctement, vous avez le droit à l'oubli mais pas le droit à l'erreur. Une seule demande par URL sera acceptée, si vous vous trompez vous ne pourrez pas revenir en arrière (en tous les cas chez Google). Rédigez soigneusement votre texte de justification qui sera lu par les équipes juridiques des moteurs. Pour vous faciliter cette étape Forget.me vous propose des textes adaptés à de nombreux cas, rédigés par des avocats. Vous pouvez soumettre plusieurs demandes uniquement dans le cas où celles-ci concernent des URL différentes.

Frontière entre personne publique et personne privée

Si vous êtes une personne publique vous ne pouvez pas prétendre à une demande de droit à l'oubli. Cependant, la frontière entre personne publique et personne non publique est encore floue. Si vous êtes une star de cinéma, il est évident que vous serez considéré comme une personne publique. En revanche, si vous êtes le maire d'une petite commune ou encore le dirigeant d'une PME, la réponse est moins évidente. Cette question se précisera sans doute dans les prochains mois, grâce aux nombreux cas que les moteurs de recherche vont devoir traiter, le travail du G29 et d'éventuelles jurisprudences ou lois à venir.

Deux formulaires de droit à l'oubli Internet disponibles : Google et Bing

Pour le moment, seul Google et Bing ont mis en place un formulaire permettant de soumettre vos demandes de droit à l'oubli. Cependant, il est probable que les autres moteurs de recherche, comme Yahoo par exemple, prévoient de proposer leur propre formulaire. Forget.me vous fait gagner du temps en soumettant votre demande simultanément à Google et Bing.

Le formulaire de droit à l'oubli Internet : un premier niveau de recours

La demande via le formulaire d'un moteur de recherche n'est qu'un premier niveau de recours. Si vos demandes sont refusées vous pouvez également vous adresser à la CNIL ou encore saisir la justice de votre pays.



Le droit à l'oubli Internet se matérialise aujourd'hui par un processus pratique et facile d'accès. Ce qui permet à chacun d'entre nous de bénéficier du droit à l'oubli. Sachant que 75%1 des citoyens européens souhaitent pouvoir exercer un droit à l'oubli, c'est une démarche qui pourrait bien rentrer dans nos habitudes.

1 Enquête Eurobaromètre portant sur les attitudes des citoyens à l'égard de la protection des données et de l'identité électronique, publiée par la Commission européenne (http://europa.eu/rapid/press-release_IP-11-742_fr.htm?locale=en)

Cet article vous a plu ? Laissez-nous un commentaire (Source de progrès)

Source :

<http://www.economiematin.fr/news-droit-oubli-google-fonctionnement-traitement-demande>
<http://www.reputationvip.com/fr/blog/infographie-le-droit-a-loubli-comment-ca-marche>

Google « discrédite » le droit à l'oubli, selon la

Cnil



Google
« discrédite »
le droit à
l'oubli, selon
la Cnil

Dans un entretien au Figaro, Isabelle Falque-Pierrotin, présidente de la Commission nationale informatique et libertés, juge sévèrement l'attitude de Google dans l'application du droit à l'oubli.

Si Google a l'obligation, suite à une décision de justice européenne, d'appliquer le droit à l'oubli pour les internautes qui en font la demande, ses méthodes ne font pas l'unanimité. Le moteur a d'ailleurs été récemment condamné par le Tribunal de Grande Instance de Paris à retirer les contenus diffamatoires de ses résultats de recherche.

Google fera probablement appel de cette décision, la question de la portée des déréférencements étant un sujet de débat entre l'entreprise et les différentes Cnil européennes.

La Cnil française justement juge assez sévèrement l'attitude de Google en la matière. Dans un entretien au Figaro, Isabelle Falque-Pierrotin, présidente de la Commission nationale informatique et libertés explique : « Les demandes d'effacement sont prévues par la loi depuis longtemps et sont appliquées par les possesseurs de sites. Google n'était pas considéré comme responsable du traitement de données personnelles ».

Replacer la Cnil au coeur du dispositif

Et d'asséner : « Il y a beaucoup d'habileté et de malice de la part de Google pour entretenir la confusion et discréditer ce droit à l'oubli. Il faut se positionner dans ce débat sans ouvrir le front des menaces de censure. Le droit au déréférencement est complexe. Il faut trouver un équilibre, avec finesse ».

Rappelons que jeudi 25 septembre 2014, s'est tenu à Paris une réunion organisée par Google sur cette question. La Cnil y a assisté en tant qu' »observateur ».

La Commission rappelle d'ailleurs qu' »en cas de refus de Google, les Français peuvent saisir la Cnil d'une plainte, en décrivant leur demande et la réponse qu'il ont obtenue. Nous avons reçu une soixantaine de plaintes, que nous allons examiner, avant d'ordonner ou non à Google de retirer ces liens. Nous avons toutefois demandé à ces personnes de patienter, car nous souhaitons nous coordonner avec les autres autorités européennes, pour définir des règles communes ».

Replacer la Cnil au centre de l'exercice du droit à l'oubli est aussi une volonté du gouvernement. Interrogée par ZDNet.fr, Axelle Lemaire, secrétaire d'Etat au Numérique souligne : « Le rôle de la CNIL doit être redéfini, le modèle proposé par Google ne me convient pas ».

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

<http://www.zdnet.fr/actualites/google-discredite-le-droit-a-l-oubli-selon-la-cnil-39806871.htm>

Droit à l'oubli : Google condamné par le TGI de Paris



Droit
l'oubli
Google
condamné
le TGI
Paris
à :
par
de

Le Tribunal de Grande Instance de Paris a condamné Google dans le cadre d'une affaire ayant trait au droit à l'oubli, rapporte Nextinpact. Cette affaire opposait Google à deux victimes de diffamation qui avaient précédemment eu gain de cause mais souhaitaient faire retirer la page Facebook incriminée des résultats de recherche.

Le 13 mai, les victimes avaient demandé à Google de déréférencer la page jugée fautive, puis face à l'absence de réaction de la part de la firme, avaient opté pour un recours en justice.

Si Google a rappelé l'existence d'un formulaire en ligne pour ce type de demandes, Nextinpact rapporte que l'avocat des victimes a souhaité ne pas avoir recours à ce procédé, qualifié de « boîte noire » laissant à Google seul juge de la validité de la demande. Compte tenu du fait que les victimes étaient parvenues à obtenir une condamnation de la page fautive pour diffamation, on comprend les réticences de l'avocat à laisser le fin mot de l'affaire entre les mains de Google.

Le bal des jurisprudences peut commencer

Le jugement du TGI de Paris a donc finalement tranché en défaveur de Google, s'appuyant sur la décision rendue par la Cour de Justice de l'Union Européenne dans l'affaire ayant mis en place le droit à l'oubli. Le moteur de recherche a donc été condamné à retirer les contenus diffamatoires de ses résultats de recherche.

Si Google a dans un premier temps cherché à circonscrire cette décision aux seuls résultats de Google France, la magistrate a néanmoins préféré demander un déréférencement mondial, compte tenu du fait que les différentes versions de Google sont accessibles depuis n'importe quel pays.

Si en terme de volume de demandes, le droit à l'oubli semble se diriger lentement mais surement vers une stabilisation, sur le terrain du droit tout reste encore à faire.

Google fera probablement appel de cette décision, la question de la portée des déréférencements étant un sujet de débat entre l'entreprise et les différentes Cnil européennes. La polémique sur le principe même du droit à l'oubli n'est aujourd'hui plus la question : ce qui importe c'est de savoir comment appliquer ce droit et quelles en sont les limites. Et sur ce terrain, les jurisprudences issues d'affaires de ce type seront déterminantes.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

<http://www.zdnet.fr/actualites/droit-a-l-oubli-google-condamne-par-le-tgi-39806739.htm>
Louis Adam

Après le BYOD, voici le WYOD

	Après Le BYOD (bring your own device), voici le WYOD
---	--

En ce mois de septembre, la principale nouvelle dans le secteur high-tech a été de loin l'annonce de l'Apple Watch. Disponible au début de l'année prochaine, la montre pourrait faire exploser le marché des produits vestimentaires connectés. De quoi développer le Wear Your Own Device (WYOD).

Un phénomène qui pourrait bien se généraliser

La future Apple Watch va-t-elle connaître le succès ? Difficile à dire pour le moment. Ce que nous savons par contre, c'est que de nombreux constructeurs et fabricants misent sur les objets vestimentaires connectés / intelligents. Que ce soit les bracelets sportifs de Nike et Fitbit ou encore les montres de Sony, Samsung, Motorola et bientôt Apple, la mode est au connecté.

En entreprise ou encore dans les établissements scolaires, nous connaissons déjà le BYOD (Bring Your Own Device), le BYOS (Bring Your Own Software) ou encore le BYOPC (Bring Your Own PC). Voici donc le WYOD, Wear Your Own Device. Bien entendu, un tel phénomène est loin d'être encore aussi grand que l'utilisation du smartphone en entreprise. Il n'empêche qu'il faut s'y préparer, car les logiques sont les mêmes.

Dorénavant ou tout du moins d'ici quelques mois ou années, il faudra donc veiller à ce que les montres connectées ne deviennent pas problématiques pour la sécurité des données sensibles de la compagnie. Et nous ne parlons même pas des lunettes connectées de Google qui peuvent être pires encore.

Bientôt invisibles à nos yeux

Les montres connectées ont de cela de spéciales que si l'on n'y prend pas garde, on ne la différenciera pas des autres montres, et donc on ne la remarquera pas. Même logique pour les vêtements connectés ou même les perruques connectées (oui oui). Bien plus difficiles à vérifier qu'un smartphone, une tablette tactile et bien entendu un ordinateur, tous ces nouveaux et futurs produits peuvent devenir le cauchemar des patrons et des DSI s'ils ne prennent pas les dispositions adéquates.

Comme le notait il y a quelques Kevin Noonan, analyste pour Ovum, les produits connectés comme les montres ou les lunettes pouvaient à l'époque paraître bizarres et étaient immédiatement identifiables. Aujourd'hui à force de les voir et de les côtoyer, ils risquent d'être invisibles à nos yeux.

Que faire ? Les interdire ?

Dans certains lieux vraiment sensibles, ce serait peut-être la solution la plus simple. Néanmoins, on a déjà vu que de nombreuses entreprises interdisaient le BYOD, ce qui n'empêchait pas les employés d'apporter leurs propres appareils, en le cachant aux yeux de leurs dirigeants. Une véritable catastrophe qu'il convient d'éviter pour les objets connectés.

Le contrôle avant tout

Plutôt qu'interdire, mieux vaut donc disposer d'une véritable politique propre à tous les appareils, y compris donc les objets et vêtements intelligents et connectés. Mieux vaut ainsi avoir le contrôle et la mainmise sur ce type de produits qu'en ignorer la présence, ce qui est la pire des situations. Qui plus est, comme pour les smartphones, les entreprises doivent en tirer profit, que ce soit pour communiquer avec leurs employés ou encore trouver un moyen d'exploiter ces objets vis-à-vis des clients. Après tout, il s'agit de produits souvent compatibles avec d'autres appareils, et il n'est pas rare qu'un important espace de stockage en ligne (cloud) l'accompagne. Si cela peut devenir un problème, cela peut donc surtout être un atout.

Il faut de plus comprendre qu'à l'heure actuelle, il n'existe pas de solutions spécifiques de sécurité pour ces objets. Stephen Brown, directeur de la gestion des produits mobiles chez Landesk, expliquait par exemple en avril dernier qu'en réalité, la première préoccupation vis-à-vis de ces produits n'est pas la sécurité mais le respect de la vie privée. C'est en particulier le cas des lunettes connectées, mais pas uniquement. Est-ce que ces appareils enregistrent constamment voire à notre insu ? Répondre à ces questions est déjà un point fondamental.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

<http://www.zdnet.fr/actualites/apres-le-byod-voici-le-wyod-39806705.htm>

Par Nil Sanyas