Après JP Morgan, 9 autres banques auraient été piratées

Après JP Morgan, 9 autres banques auraient été piratées

Le groupe responsable du piratage de JP Morgan cet été aurait mené des attaques sur 9 autres établissements financiers. Comme la loi américaine n'oblige pas les banques à communiquer sur ce genre d'incident, l'ampleur exacte de la fuite potentielle de données reste inconnue.

JP Morgan serait loin d'être la seule banque à avoir été attaquée par ce groupe de pirates. Il s'agirait en réalité d'une vague d'intrusions, dont l'ampleur exacte reste inconnue.

Elle aurait permis aux assaillants « d'infiltrer environ 9 autres établissements financiers », explique le New York Times en s'appuyant sur des sources proches de l'enquête.

De nombreux points à éclaircir

Peu de détails ont été révélés par les canaux officiels. D'ailleurs, le journal américain n'a pas pu obtenir les noms des établissements infiltrés et ignore toujours ce à quoi les pirates ont pu accéder.

JP Morgan, seule banque à avoir communiqué sur le sujet, affirme que les responsables n'ont pu accéder qu'aux noms des clients et à d'autres informations non-financières. Le personnel chargé de la sécurité de la banque aurait repéré l'attaque avant que les assaillants n'accèdent aux données sensibles. Ceci étant dit, l'intrusion n'aurait pas été entièrement arrêtée avant la mi-août alors qu'elle avait débuté en juillet.

Pour ce qui est de l'identité des pirates, les autorités en charge de l'enquête pencheraient pour un groupe opérant depuis la Russie. Ils auraient une « vague connexion » avec des membres du gouvernement de Moscou.

Les motivations des pirates restent, elles aussi, inconnues. Cependant, ces attaques pourraient avoir été menées en représailles aux sanctions visant la Russie dans le cadre de la crise ukrainienne, présument les services de renseignement américains.

Une brèche dans les systèmes mais aussi dans la loi ?

Outre l'aspect sécuritaire, l'attaque met en évidence une potentielle lacune dans la loi américaine. On apprend aujourd'hui que l'incident a bien plus d'ampleur qu'il n'y parait. Peut être qu'une meilleure information aurait permis de limiter l'intrusion ou d'aider à faire avancer l'enquête. Seulement, les banques en ligne ne sont pas obligées de communiquer sur les événements ayant pu compromettre les données des clients à moins qu'ils leur aient fait perdre de l'argent.

Dans certains Etats américains, les banques peuvent attendre jusqu'à un mois avant d'informer les autorités et les clients de ce type d'incident. La loi californienne, par exemple, impose simplement un délai « raisonnable », une définition sujette à interprétations. Il est alors difficile, dans un tel contexte, de lutter efficacement contre ce type de piratage.

La France n'est pas mieux lotie : les banques ne sont pas tenues d'informer les clients lors d'une fuite de données. Pour l'instant, seuls les fournisseurs d'accès et opérateurs ont l'obligation de notifier la CNIL ou les clients. Cependant, le régulateur français et ses équivalents européens cherchent à étendre ces exigences à l'ensemble des services en ligne.

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

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-731231-jp-morgan-9-banques-attaquees-pirates.html

500 000 PC infectés à cause d'une faille Windows XP

500 000 PC infectés à cause d'une faille Windows XP

Selon les chercheurs en sécurité de Proofpoint, 52% des PC infectés par le botnet Qbot font tourner Windows XP. Exploitant une faille de Windows XP mais également de Seven et Vista, un groupe de cybercriminels russe a réussi à activer le botnet Qbot fort 500 000 PC zombies, essentiellement localisés aux Etats-Unis. Son objectif : Aspirer les identifiants bancaires des utilisateurs de ces PC corrompus.

Des pirates russes à l'origine du botnet Qbot ont construit une impressionnante armée de 500 000 PC zombies en exploitant des failles non corrigées dans des ordinateurs tournant sous Windows XP mais également Windows 7 et Vista. Des PC localisés principalement aux Etats-Unis, a fait savoir la société Proofpoint. Ces derniers temps, les hackers russes ont fait monter la pression avec des incursions sérieuses telle que l'attaque qui a visé la banque américaine JPMorgan Chase. Avec ce botnet, baptisé Qbot, les chercheurs de Proofpoint ont fait ressortir que le groupe qui est à l'origine de sa création l'a élaboré de façon méticuleuse à travers le temps, sans faire de vague, au point de rester sous les radars des sociétés de sécurité et donc de ne pas avoir attiré leur attention.

Selon Proofpoint, 75% des 500 000 PC infectés par le botnet Qbot sont situés aux Etats-Unis, sachant que parmi eux, 52% font tourner Windows XP, 39% Windows 7 et 7% Windows Vista. En Grande-Bretagne, la proportion de PC infectés est bien moindre, 15 000 postes environ. « Avec 500 000 clients infectés volant les identifiants des comptes bancaires en ligne des utilisateurs, le groupe de cybercriminels a le potentiel pour réaliser des bénéfices vertigineux », ont indiqué les chercheurs de la société de conseil en sécurité. Mais le botnet Qbot ne s'attaque pas seulement aux comptes bancaires, il compromet également les sites WordPress, soit en infectant le site lui-même ou bien en injectant des contenus corrompus dans leurs newsletters.
Article de Dominique Filippone

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

Source :
http://www.lemondeinformatique.fr/actualites/lire-500-000-pc-infectes-a-cause-d-une-faille-windows-xp-58878.html

Un nouveau malware vise les Mac, 17.000 machines affectées ?

Un nouveau malware vise les Mac, 17.000 machines affectées ?

Selon la firme russe Dr.Web un malware visant spécifiquement les possesseurs de Mac serait actuellement actif, affectant plus de 17.000 machines à travers le monde. Pas une première, mais ce malware possède quelques spécificités amusantes.

Pas la peine de se mentir, les produits Apple eux aussi sont parfois victimes de malwares. En 2011, le Trojan Flashback avait ainsi infecté des centaines de milliers d'ordinateurs Apple. Le malware détecté par Dr Web est en revanche bien moins diffusé : 17.000 utilisateurs seulement seraient infectés.
Ce malware se range sous la catégorie des Botnets, infectant l'ordinateur de l'utilisateur afin de permettre à l'attaquant de l'exploiter pour d'autres fonctions à l'insu de son utilisateur. Le malware a été baptisé, un peu rapidement, iWorm par Doctor Web, bien que le mode exact de propagation du virus reste encore peu clair.
La particularité qui a retenu l'attention des chercheurs, c'est la façon dont les ordinateurs infectés récupèrent les adresses IP des serveurs de command&control. Les machines du botnet vont ainsi chercher sur Reddit les adresses de leurs centre de command&control : celles-ci sont postées à intervalles régulier dans la section commentaire d'un sujet destiné à recenser des serveurs Minecraft via un compte tenu par les individus responsables de la propagation du malware.

Reddit est innocent !
Reddit n'a rien à se reprocher, le site n'a pas été altéré ou son utilisation n'a pas été techniquement détournée, mais cette approche originale mérite d'être notée. Comme le relève le chercheur Graham Cluley, même en supprimant le compte utilisé pour router vers ces adresses IP, cela n'empêcherait pas les pirates de recréer un compte et de continuer leur activité.
Comme souvent néanmoins, il convient de rester prudent avec les alertes lancées par les firmes spécialisées dans la vente d'antivirus. Dr.Web annonce ainsi 17.000 ordinateurs infectés à travers le monde, mais ne précise pas du tout quel mode de diffusion a été choisi pour propager le malware. Selon des sources anonymes, le principal mode d'infection se ferait via le téléchargement de logiciels Adobe et Microsoft piratés sur les plateformes de partage en P2P.
De la même manière, peu d'informations sont disponibles pour ceux qui souhaitent se prémunir de ce malware, si ce n'est la solution vendue par Dr.Web… Mais selon MacRumors, l'outil de protection maison proposé par Apple à ses clients Xprotect, a été mis à jour pour détecter et empêcher la propagation de cette menace.
Attention Livo !

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

Source :
http://www.zdnet.fr/actualites/un-nouveau-malware-vise-les-mac-17000-machines-affectees-39807339.htm
Par Louis Adam | Lundi 06 Octobre 2014

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, agés 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 ?
Informer 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 à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/legislation-loi-internet/cnil/actualite-730529-cnil-controles-rappel-commercants.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.

Une première voiture imprimée en 3D, la Strati, a vu le jour

	Une première voiture imprimée en 3D, la Strati, a vu le jour

Il ne s'agit pour l'instant que d'un prototype mais il roule. Le PDG à l'origine de cette première mondiale espère bien en vendre d'ici à la fin de l'année.

Il n'a fallu que 44 heures pour imprimer la Strati.
Après les armes à feu et les pizzas, voici venir la voiture imprimée en 3D : la Strati. Cette première mondiale est l'œuvre d'une entreprise américaine, Local Motors, et a eu lieu lors d'un salon des technologies de l'industrie à Chicago.
Le design de ce véhicule a été choisi parmi 200 propositions faites par des internautes au constructeur à l'annonce de ce projet en avril dernier. Il a fallu 44 heures à Local Motors pour imprimer les 40 éléments de la Strati (contre une moyenne de 20 000 pour un véhicule classique), à partir de billes de plastique thermoformé renforcé de fibres de carbone.
Ils ont ensuite été assemblés avec d'autres éléments conçus de manière traditionnelle (comme les roues, les suspensions, le moteur et le pare-brise).
Ce petit buggy électrique biplace peut atteindre la vitesse de 40 miles à l'heure (environ 65 km/h) et dispose d'une autonomie de 120 miles en une charge. La Strati a même roulé prouvant que le véhicule était parfaitement opérationnel.

Local Motors espère vendre ses strati d'ici à la fin de l'année 2014.

Le constructeur envisage d'imprimer de petites séries de cette voiture d'ici à la fin de l'année pour un tarif démarrant à 18 000 dollars (13 929 euros). « Dans les prochains mois, nous espérons descendre sous la barre des 24 heures, voire celle des 10 heures (temps nécessaire actuellement pour construire une voiture classique) », a expliqué le PDG de Local Motors, John Rogers, à l'occasion de ce salon. Pour le dirigeant, ce véhicule marquera « un tournant dans l'industrie automobile ».

<iframe width= »560″ height= »315″ src= »//www.youtube.com/embed/daioWlkH7ZI » frameborder= »0″ allowfullscreen></iframe>

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

Source :
http://www.01net.com/editorial/626842/une-premiere-voiture-imprimee-en-3d-la-strati-a-vu-le-jour/#?xtor=EPR-1-NL-01net-Actus-20140915
Cécile Bolesse

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 ?

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 inexactes, 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 garantie 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 le 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 »références : 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