

Menacé de chantage sur Skype, un lycéen se suicide | Le Net Expert Informatique



Menacé de chantage sur
Skype, un lycéen se
suicide

Après avoir été menacé par son interlocutrice virtuelle de voir une « vidéo intime » diffusée sur Internet s'il refusait de la payer, un jeune homme s'est donné la mort dans sa chambre.

Mercredi 4 juin, un peu avant 20 heures, à Castelsarrasin (Tarn-et-Garonne), un lycéen de 18 ans – qui s'appellerait Quentin – est attendu à la table familiale pour dîner. En l'absence de réponse à leurs appels, ses parents se rendent dans sa chambre. Et le découvrent dans une mare de sang, un couteau planté en plein cœur. Quentin est déclaré mort peu après l'arrivée des secours. Les policiers qui leur font suite se concentrent sur son ordinateur portable, resté allumé. Ils y découvrent les causes probables de son suicide grâce à la fenêtre de conversation restée ouverte sur sa messagerie vidéo Skype : un chantage à la webcam.

Une jeune femme le menace de diffuser une vidéo intime

Les enquêteurs remontent le fil de la discussion et constatent que Quentin s'était filmé nu pour son interlocutrice. Celle-ci l'avait ensuite menacé de diffuser cet enregistrement sur internet s'il refusait de payer une certaine somme d'argent sur le champ. Pris de panique, Quentin se serait donné la mort pour éviter un scandale. Le parquet de Montauban a ouvert une enquête préliminaire.

« La Dépêche du midi », qui avait d'abord évoqué l'hypothèse d'un chagrin d'amour avant de retenir celle du chantage, précise que la mère du lycéen l'aurait découvert avec une « corde au cou ». Mais évoque également, comme RTL, une « mare de sang ».

Le jeune homme, décrit comme un « très bon élève » de terminale au lycée professionnel de Beaumont-de-Lomagne, n'avait jamais parlé de suicide à ses proches. Les centres d'intérêt de son probable profil Facebook tournaient essentiellement autour des mangas.

Un scénario similaire à Brest, en 2012

Ce suicide rappelle un drame similaire survenu à Brest en octobre 2012. Un jeune homme de 18 ans s'était dénudé par webcam, sur Facebook, à la demande d'une jeune femme rencontrée en ligne qui faisait de même. Avant d'interrompre le « jeu » au bout de 10 minutes en le menaçant : « J'ai une vidéo porno de toi, si tu ne me donnes pas 200 euros, je vais détruire ta vie. »

Paniqué à l'idée de voir la vidéo diffusée à ses amis Facebook, le lycéen s'était pendu après avoir laissé un SMS d'adieu à ses parents. L'adresse IP de la femme provenait de Côte d'Ivoire, où des maîtres chanteurs connus sous le nom de « brouteurs » sont devenus des professionnels de ce genre de pratique.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<http://tempsreel.nouvelobs.com/faits-divers/20150605.OBS0251/menace-de-chantage-sur-skype-un-lyceen-se-suicide.html>

Par Alexis Orsini

Une imprimante 3D pour personnaliser la mousse de votre café latte | Le Net Expert Informatique



Une imprimante 3D pour
personnaliser la mousse de
votre café latte

Un support de communication inattendu développé par la startup Coffee Ripples.



L'entreprise Coffee Ripples a mis au point une machine qui permet d'écrire le message de votre choix sur la mousse d'un café : The Ripple Maker. Un site et une app mobile permettent d'uploader et adapter le message désiré. Celui-ci est alors imprimé sur la surface de la boisson en poudre de café, combinant ainsi les technologies de l'impression 3D et du jet d'encre. Coffee Ripples mise sur un prix de vente de 999 USD avec un abonnement annuel de 75 USD pour permettre aux commerces d'utiliser pleinement toutes les fonctionnalités et s'attirer le capital sympathie des clients. Retrouvez plus d'information sur le site de de la startup.

Coffee Ripples profite ainsi d'un emplacement peu investi pour communiquer, tout en surfant sur un art de plus en plus populaire. Il suffit pour cela de jeter un œil au hashtag #latteart sur Instragram. Lufthansa a d'ores et déjà signé pour cette technologie dans le but d'imprimer le logo de la compagnie sur les cafés des voyageurs de première classe.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://lareclame.fr/132138-coffee-ripples-un-cafe-pour-instagram-sans-filtre>

Première forte condamnation pénale d'atteinte à la E-réputation | Le Net Expert Informatique



Première forte condamnation pénale d'atteinte à la E-réputation

L'excellent site [Légalis.net](http://www.legalis.net) vient de rendre public un jugement du Tribunal correctionnel de Paris en date du 24 novembre 2014, qui a condamné à 2 ans de prison avec sursis, 3 ans de mise à l'épreuve ainsi que 50 000 € de dommages-intérêts à verser aux victimes et 27 000 € pour participation aux frais de justice des plaignants.

Les faits en bref

Il s'agit d'une femme qui n'a pas supporté d'être quittée par son amant. Elle s'est donc déchaînée contre lui, en n'hésitant pas à user de toute la technique d'internet pour usurper son identité et créer à son nom des comptes sur des réseaux sociaux (Facebook, Viadeo, LinkedIn, Twitter), harcelant sa famille, sa nouvelle compagne et même l'employeur de cet homme, ainsi que de nombreux autres agissements tels que du harcèlement téléphonique, montrant pour le moins le manque de stabilité psychologique de l'intéressée.

L'affaire avait été classée par le Procureur de la République sous la condition que la personne se tienne tranquille, ce qu'elle a été incapable de faire et elle a continué ses agissements nuisibles, d'où les poursuites et cette lourde condamnation.

Quant la méchanceté rejoint la lâcheté

Ce cas d'espèce n'est pas aussi particulier ni exceptionnel qu'on pourrait le penser. Même si les faits ne sont pas toujours portés devant la justice et médiatisés, notre expérience de nettoyeurs de net nous apporte de nombreux cas de réel acharnement de personnes qui ont le goût de nuire ou la haine suffisants pour chercher à détruire des personnes, par exemple à démolir la vie de la femme qui a osé demander le divorce contre eux, ou encore qui se sont juré qu'ils auraient la peau d'un dirigeant d'entreprise en proférant les plus graves accusations non fondées et qui continuent à le faire, sur des sites hébergés à l'étranger, alors même qu'ils sont déjà lourdement condamnés pour diffamation en correctionnelle puis en appel.

La technique du pseudonyme – ou ici celle de l'usurpation d'identité – donne très souvent aux personnes malfaisantes l'impression grisante de puissance et d'impunité (voir notre actualité du 26 février 2010 : Sur le Web 2.0 c'est carnaval tous les jours). Ce qui permet ainsi de nuire en toute impunité et en toute lâcheté...

Il y a encore la possibilité de publier sur des sites hors d'atteinte du droit français, ce qui rend les choses encore plus compliquées et plus longues à neutraliser. Mais il faut savoir qu'une telle neutralisation, même si elle est plus longue, est rarement impossible.

Dans le cas de la jurisprudence que nous évoquons, on a eu affaire à une personne suffisamment instable et incontrôlable pour qu'elle laisse des traces et qu'on remonte très vite à son identité. Mais les cas sont hélas fréquents où il est impossible d'identifier rapidement l'auteur de telles manœuvres de démolition. Il faut alors saisir la justice, avec tous les délais et les frais que cela suppose pour que, au cours de l'enquête, le juge ordonne des mesures pour remonter jusqu'à l'auteur des faits, notamment par voie d'injonction aux hébergeurs ou aux opérateurs de réseaux.

Une décision de justice exemplaire

Malgré ces réserves, il faut saluer cette décision de justice comme exemplaire au sens fort du terme : elle doit servir d'exemple pour toute personne qui serait tentée de nuire avec autant d'acharnement contre des personnes.

L'affaire reste à suivre car le jugement a été frappé d'appel : on aura donc sans doute prochainement des nouvelles de ce cas et la confirmation ou l'infirmité de la sentence par la Cour d'appel de Paris.

Le jugement : http://www.legalis.net/spip.php?page=breves-article&id_article=4672

La décision de justice intégrale : http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4671

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<http://www.les-infostrategies.com/actu/15072025/e-reputation-premiere-forte-condamnation-penale-assortie-de-dommages-interets>

Une loi pour vous espionner... | Le Net Expert Informatique



Une loi
pour vous
espionner...

Alors que les révélations sur les activités de la NSA en France se multiplient et que le terrorisme frappe à nouveau, le gouvernement vient de faire voter une loi sur le renseignement qui autorise de nouvelles techniques d'espionnage très intrusives. Enquête sur ces nouveaux dispositifs controversés.

«Inacceptables.» C'est en ces termes attendus que l'Elysée a qualifié les écoutes de l'agence américaine NSA sur la France, révélées à partir du 24 juin par l'organisation WikiLeaks et les journaux Mediapart et Libération. L'ensemble de la classe politique a réagi à l'unisson aux premières publications de documents concernant les interceptions par la NSA, entre 2006 et 2012, des conversations des trois présidents successifs Jacques Chirac, Nicolas Sarkozy et François Hollande, ainsi que des cas d'espionnage économique. «Ces pratiques portent atteinte à la confiance entre alliés», a fustigé le ...
Lire la suite...

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<http://www.lefigaro.fr/actualite-france/2015/07/03/01016-20150703ARTFIG00179-loi-renseignement-comment-vous-allez-etre-espionnes.php>

Reconnaissance faciale, une menace pour la vie privée ? | Le Net Expert Informatique



Reconnaissance faciale, une menace pour la vie privée ?

Pour le «Washington Post», les nombreuses applications capables de reconnaître les visages créent des bases de données biométriques dangereuses pour la «confidentialité numérique».

«L'anonymat en public pourrait être une chose du passé.» Dans le Washington Post du 11 juin, Ben Sobel, chercheur au Centre sur la vie privée et la technologie de l'école de droit de Georgetown, consacre un article au risque qui pèse sur notre «confidentialité biométrique». Selon lui, les technologies de reconnaissance faciale se développent à la vitesse grand V sous l'impulsion du marketing individualisé. Et pas toujours de manière très légale.

Aux Etats-Unis, Facebook fait l'objet d'un nouveau procès en action collective, concernant la violation du droit à la protection des données personnelles de ses utilisateurs. En cause, le réseau social serait en train de créer «la plus grande base de données biométriques privées au monde» sans demander assez explicitement le consentement de ses utilisateurs comme l'explique le site Sophos. Le gouvernement américain et le département du Commerce auraient déjà invité des associations de défense de la vie privée ainsi que des représentants des grandes entreprises de ce secteur comme Google et Facebook pour essayer de réglementer l'usage de ces technologies.

Mais pour le moment, seul l'Illinois (2008) et le Texas (dès 2001) ont des lois interdisant l'utilisation de cet outil sans le «consentement éclairé» des utilisateurs, explique Ben Sobel. Selon lui, l'issue de ce procès, qui devra déterminer si Facebook a enfreint la «Biometric Information Privacy Act» (BIPA) de l'Illinois, déterminera l'avenir des applications de reconnaissance faciale sur le marché. Il encourage ainsi les Etats-Unis à adopter une loi fédérale pour garantir la «confidentialité biométrique» des Américains.

LE BOOM DES APPLICATIONS DE RECONNAISSANCE FACIALE

FaceNet (Google), Name Tag (FacialNetwork) ou encore Moments (Facebook). Toutes ces applications utilisent des algorithmes de reconnaissance faciale. Et pour les imposer sur le marché, les entreprises sont prêtes à tout pour mettre leur adversaire échec et mat.

FaceNet, la technologie développée par le géant Google, possède une précision de 99,63 % selon Ben Sobel. Elle est actuellement utilisée par Google Photos dans ses versions non européennes. Dans la même lignée, Name Tag, développé par FacialNetwork, ambitionne de fonctionner sur les Google Glass. Cette application permettrait de rassembler tous les profils sur les réseaux sociaux disponibles sur Internet (Twitter, Instagram, Google+ et sites de rencontres américains) selon un article du Huffington Post. Une application qui pourrait permettre d'avoir le profil social de quelqu'un en temps réel.

Parmi les fonctionnalités envisagées, il y aurait par exemple celle de révéler la présence de quelqu'un dans les bases de données criminelles. Pour le moment, Google a refusé que NameTag soit disponible sur ses Google Glass, pour des questions de problèmes de respect de la vie privée... Mais il n'est pas le seul à s'engouffrer dans ce marché.

Depuis 2011, Facebook utilise un système de suggestion de tags (identifications) sur les photos. Bien qu'interdit en Europe, Deepface, l'algorithme expérimental du réseau social, serait capable de reconnaître les gens à leur posture corporelle. De fait, son algorithme utilise ce que l'on appelle des «poselets». Inventés par Lubomir Bourdev, ancien chercheur de Berkeley œuvrant désormais chez Facebook IA Research. Ceux-ci repèrent les caractéristiques de nos visages et trouvent ce qui nous distingue de quelqu'un d'autre dans une pose similaire, explique un article de Numérama (<http://www.numerama.com/magazine/33026-meme-de-dos-facebook-sait-vous-reconnaitre-sur-les-photos.html>). Mais Facebook ne s'arrête pas là. En juin, le réseau social a présenté Moments, une application permettant de partager de manière privée des photos avec des amis utilisant elle aussi une technologie de reconnaissance faciale. D'ores et déjà disponible gratuitement aux Etats-Unis, elle permet à un utilisateur d'échanger avec ses amis des photos où ils figurent de manière synchronisée. Une vidéo en explique les rouages :

Moments ne devrait pas s'exporter en Europe de sitôt, puisque l'UE exige la mise en place d'un mécanisme d'autorisation préalable qui n'est pas présent sur la version américaine. Et ce, bien que les utilisateurs puissent désactiver les suggestions d'identification sur les photos, via les paramètres de leur compte.

L'INQUIETUDE AUTOUR DU SUCCÈS DE CES TECHNOLOGIES

En 2012, une recommandation formulée par le G29, qui réunit les commissions vie privée de 29 pays européens, mettait déjà en garde contre les dangers de la reconnaissance des visages sur les médias sociaux. Notamment concernant les garanties de protection des données personnelles, tout particulièrement les données biométriques. Pour le moment relativement bien protégés par la législation européenne, nous ne sommes pas pour autant épargnés par ces outils.

Tous les jours, 350 millions de photos sont téléchargées sur Facebook, selon Ben Sodel. Or, le public semble majoritairement insouciant face à la diffusion de son identité (nom, image...), souligne InternetActu. A l'exemple de l'application How Old mise en ligne fin avril, qui se targue de deviner votre âge grâce à une photo. Corom Thompson et Santosh Balasubramanian, les ingénieurs de Microsoft à l'origine du projet, ont été surpris de constater que «plus de la moitié des photos analysées» par leur application n'étaient pas des clichés prétextes mais de vraies photos, rapporte le Monde.

Mais le succès (bien qu'éphémère) de cette application démontre bien que le public n'est pas vigilant face à la généralisation de la reconnaissance faciale. Un peu comme avec la diffusion des données personnelles au début de Facebook. Il ne s'agit pas tant du problème de stocker des photos d'individus que de mémoriser l'empreinte de leur visage. Entre de mauvaises mains, ces bases de données pourraient mettre à mal notre «confidentialité biométrique».

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous
Denis JACOPINI
Tél : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

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

Source : http://ecrans.liberation.fr/ecrans/2015/06/26/reconnaissance-faciale-une-menace-pour-la-vie-privée_1337015
Par Camille PETTINEO

Les techniques du renseignement français se dévoilent un peu plus | Le

Net Expert Informatique



Les techniques du
renseignement français se
devoient un peu plus

Le Nouvel Obs a publié dans ses colonnes une longue enquête faisant le point sur les écoutes et techniques mises en place par le renseignement français. Un rapide aperçu des capacités de la France en la matière.

Et le premier constat que l'on peut tirer, c'est que la France s'est évertuée à rattraper son retard sur les américains dès 2008. Comme le rapporte l'Obs, c'est en effet à cette date qu'a été lancée la première phase d'un plan initié par Nicolas Sarkozy afin de remettre en adéquation les méthodes et équipement des services de renseignement français, dont l'essentiel des ressources s'était concentré dans les années 80 et 90 sur l'interception des communications satellites.

Des satellites aux câbles

Plus intéressants que les communications satellites en effet, les câbles sous-marins sont devenus au cours de la première décennie des années 2000 l'axe privilégié de transit d'informations. Et comme le remarquaient certains observateurs, la France est particulièrement bien située à cet égard, disposant à la fois de nombreux câbles en direction de l'Afrique du Nord, ainsi qu'à travers le Pacifique ou la Méditerranée. Et dispose en plus de cela d'un acteur majeur du marché, Alcatel, qui selon l'Obs a participé à la mise en place de cette surveillance du réseau en formant les services du renseignement aux techniques de manipulation de la fibre.

Orange serait aussi venu prêter main-forte, l'opérateur gère en effet l'accès aux points d'arrivée de ces câbles sous-marins en France, qui en dénombre une douzaine. La technique utilisée n'a rien de révolutionnaire : il s'agit de l'extension numérique de la technique des « bretelles » : une ligne dédoublée, dont l'une des extrémités part directement vers un local de la DGSE.

L'Obs détaille le régime auquel ces écoutes étaient soumises : la Commission nationale de Contrôles des Interceptions de Sécurité avait ainsi son mot à dire, et des règles étaient posées afin d'éviter les abus, notamment à l'égard des citoyens français. Mais face aux réalités et à l'ampleur du phénomène, la CNCIS se contentait de donner un avis par pays pour autoriser ou non les écoutes, simplifiant l'acheminement des données vers un datacenter dédié au traitement situé à Paris, boulevard Mortier. L'organe de contrôle, aujourd'hui remplacé par la CNCTR dans le cadre de la loi Renseignement, pouvait aussi décider de limiter les écoutes à un thème précis.

Des écoutes encadrées ?

L'hebdomadaire rapporte que les écoutes se focalisaient sur certains pays, tels que les États-Unis ou le Moyen-Orient, et en délaissaient d'autres, comme le Japon. Le magazine souligne également le fait que ces écoutes n'ont pas été simplement employées dans le cadre de la lutte antiterroriste, mais aussi pour la promotion économique du pays. Une révélation qui peut faire sourire, alors que Wikileaks a révélé en début de semaine les indiscrétions de la NSA sur ces questions. On se demande même si ces révélations ne tombent pas à pic...

L'Obs donne les contours d'un vaste plan engagé par le renseignement français : en l'espace de 5 ans, à compter de 2008, 700 millions d'euros ont été débloqués dans le cadre de ce plan et 600 embauches parmi les services. Et d'expliquer que François Hollande, lors de son arrivée au pouvoir en 2012, n'a pas remis en question cet effort et travaille au contraire à approfondir les premiers accords noués sous Sarkozy avec le GCHQ britannique, avec qui la France a établi en 2010 un traité militaire comprenant un discret volet sur l'échange d'informations dans le domaine du renseignement.

Une structure d'ampleur, que la loi Renseignement, actuellement examinée par le Conseil constitutionnel, ne vient absolument pas remettre en cause.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.zdnet.fr/actualites/les-techniques-du-renseignement-francais-se-devoilent-un-peu-plus-39821892.htm>

Par Louis Adam

L'Afrique a besoin de cybersécurité | Le Net Expert Informatique

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>L'Afrique a besoin de cybersécurité</p>
--	---

Avec un taux de croissance au niveau des TIC de l'ordre de 30% sur un marché de plus d'un milliard de personnes, l'Afrique représente le nouvel Eldorado du monde numérique.

Or, la surface d'attaque augmentant, les cybercriminels élargissent leur champ d'action. La cybercriminalité en Afrique est organisée et bien enracinée, en particulier au Nigéria, au Ghana et en Côte d'Ivoire. Désormais, l'Afrique n'est plus le théâtre des seuls cybercriminels mais aussi de cyberhacktivistes voire de hackers. Le Sénégal a été la victime de cyberattaques en janvier dernier revendiquées par le collectif anonymous du Sénégal. Par rebond des attaques massives menées en janvier en France suite aux attentats de Charlie Hebdo, les serveurs de l'agence de l'informatique de l'Etat du Sénégal sont tombés.

Devant ce désert cybernétique, les Etats d'Afrique tentent de réagir en relevant le défi de sécuriser leurs infrastructures réseau, leurs données et en formant leurs personnels. La France participe activement à la formation cyber des officiers et des techniciens par le biais de la coopération opérationnelle (ministère de la défense). Depuis 2013, une centaine d'officiers et sous-officiers ont été formés au Sénégal, au Niger et au Burkina Faso par les Eléments français au Sénégal.

Le Security Day, qui se tiendra les 15 et 16 mars 2016 à Dakar, sera l'occasion d'aborder l'ensemble de ces sujets.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : Newsletter n°3 FIC

https://www.forum-fic.com/site/FR/Newsletter/S_inscrire_a_la_newsletter,C58881,I58949.htm

La Cnil interdit la géolocalisation du salarié en dehors du temps de travail | Le Net Expert Informatique



La Cnil interdit la géolocalisation du salarié en dehors du temps de travail

Par une délibération du 4 juin 2015, la Cnil a décidé de renforcer l'encadrement du recours au dispositif de géolocalisation.

La Commission nationale de l'informatique et des libertés (Cnil) constate le développement de dispositifs dits de géolocalisation permettant aux organismes privés ou publics de prendre connaissance de la position géographique, à un instant donné ou en continu, des employés par la localisation des véhicules mis à leur disposition pour l'accomplissement de leur mission. Ainsi, l'employeur peut contrôler le respect des règles d'utilisation d'un véhicule par ses employés grâce à la géolocalisation.

Ce dispositif permet de collecter des données à caractère personnel et sont donc soumis aux dispositions de la loi du 6 janvier 1978.

Par délibération n° 2015-165 du 4 juin 2015, la Cnil a considéré qu'il était nécessaire de compléter la norme permettant de simplifier la déclaration des traitements visant à géolocaliser un véhicule utilisé par un employé.

Dans cette délibération, la Cnil précise que le recours au dispositif peut servir à justifier la réalisation d'une prestation auprès d'un client ou d'un donneur d'ordre, ou bien à lutter contre le vol du véhicule.

En outre, la Cnil interdit formellement aux employeurs de collecter des données de localisation en dehors du temps de travail du salarié, à savoir lors de ses temps de pause et du trajet entre son domicile et le lieu de travail.

La faculté de désactiver la fonction de géolocalisation doit être laissée à l'employé. Toutefois, la Cnil souligne que des explications pourront être demandées au salarié lorsque les désactivations sont trop longues ou trop fréquentes.

Enfin, les employeurs publics et privés devront se conformer au nouveau dispositif avant le 17 juin 2016.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://droit-public.lemondedudroit.fr/droit-a-entreprises/droit-social/206288-la-cnil-interdit-la-geolocalisation-du-salarie-en-dehors-du-temps-de-travail.html>

La Gendarmerie Nationale souhaite s'équiper d'une vingtaine de drones | Le Net Expert Informatique



La Gendarmerie Nationale souhaite s'équiper d'une vingtaine de drones

La Gendarmerie nationale souhaite s'équiper d'une flotte de drones, comme l'avait récemment annoncé Bernard Cazeneuve. Et c'est un appel d'offres qui a été lancé pour l'achat d'une vingtaine de drones répondant à certains critères spécifiques.

Le ministère de l'Intérieur vient de lancer un appel d'offres visant « la fourniture de microdrones au profit de la Gendarmerie nationale, le maintien en condition opérationnelle des microdrones acquis, et la formation pour la fonction de télépilote ». Plus qu'une flotte de drones, il est question des dispositifs ainsi que d'une formation à leur utilisation et leur entretien.

La Gendarmerie nationale devrait disposer de 23 appareils de la famille des « quadrirotors à décollage vertical » qui permettent un contrôle précis, une stabilité accrue, mais qui permettront le vol stationnaire pour la mise en place d'opération de surveillance.

Il sera question de 4 à 6 drones haut de gamme qui devront disposer d'un mode de vol manuel et automatique. Le drone devra être capable de voler tout seul selon un ensemble de points de passage prédéfini. Son autonomie devra être d'au moins 20 minutes avec une vitesse équivalente à un kilomètre avalé en moins de deux minutes. L'appareil devra embarquer une caméra et retransmettre ses images en direct.

Un second lot de 19 à 30 drones sera constitué de modèles plus accessibles. La Gendarmerie nationale souhaite toujours un mode de vol automatique ainsi qu'une caméra embarquée, mais ici, la question de l'autonomie et de la vitesse importent moins, puisqu'il s'agira avant tout de mener des opérations de surveillance fixe dans le cadre d'interventions de sécurisation de la voie publique.

La Gendarmerie nationale souhaite des drones fiables, équipés de zoom x10 au minimum, le tout avec un relatif silence opérationnel permettant la mise en place d'une surveillance discrète.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.generation-nt.com/gendarmerie-nationale-equipe-drones-volants-actualite-1916394.html> :

WHOIS : vos informations personnelles bientôt publiques ? | Le Net Expert Informatique

x	WHOIS : vos informations personnelles bientôt publiques ?
---	--

L'ICANN pourrait bientôt modifier le système du WHOIS. Le régulateur propose notamment d'interdire aux propriétaires de sites « à but commercial » de s'enregistrer via proxy, soit de façon anonyme. Le texte ne laisse pas les associations insensibles, qui y voient une menace pour ceux qui s'expriment librement sur leurs sites.

WHOIS est souvent décrit comme l'annuaire d'Internet. Lors de l'enregistrement d'un nom de domaine, un internaute doit renseigner diverses informations personnelles, de son état civil à son numéro de téléphone en passant par son adresse de domicile. Ces informations alimentent les bases de données des registres de noms de domaine, et sont consultables via l'outil WHOIS.

Pour des questions évidentes de protection de la vie privée et de confidentialité, les données fournies par le propriétaire d'un nom de domaine ne sont pas accessibles au public. Les registres de renseignement proposent fréquemment en option la possibilité de s'enregistrer via proxy. Les seules tierces personnes alors en mesure d'accéder aux bases de données non anonymisées sont celles détenant une autorisation légale, tel qu'un mandat judiciaire.

Mais cette situation connaîtrait ses derniers jours. L'ICANN prévoit en effet de modifier le système en profondeur. Le régulateur étudie actuellement un projet, lequel envisage notamment que les noms de domaine « utilisés dans un but commercial soient inéligibles à l'enregistrement proxy/privacy ». En d'autres termes, les propriétaires de sites contenant un quelconque élément transactionnel ne pourront plus s'enregistrer de façon anonyme : leurs informations personnelles devront être publiques.

L'anonymat, garant de la liberté d'expression

Alors que l'ICANN doit se prononcer le 7 juillet sur ce texte, l'Electronic Frontier Foundation appelle les internautes à s'y opposer. Selon l'EFF, le terme « but commercial » englobe un grand nombre de sites, et la vie privée de leurs propriétaires, des personnes physiques, seraient menacée. L'association prend pour exemple TG Storytime, un site destiné aux auteurs transgenres et hébergés par Joe Six-Pack, lui-même transgenre. Si l'ICANN devait modifier la régulation en vigueur, ses adresses, numéros de téléphone et mails seraient alors exposées à la vue de tous, trolls et harceleurs compris.

Le changement a été impulsé par les géants américains du divertissement, signale l'EFF, ce que l'ICANN ne cache pas. En effet, à de nombreuses reprises, le régulateur d'Internet écrit que cette proposition vise à faciliter le signalement de sites violant le droit d'auteur (ou toute autre propriété intellectuelle). Pour l'EFF, « ces entreprises veulent de nouveaux outils pour découvrir l'identité des propriétaires de sites Web qu'ils veulent accuser de violation de droit d'auteur et contrefaçon de marque, de préférence sans une ordonnance du tribunal ».

« L'avantage limité de cette évolution est manifestement compensé par les risques supplémentaires pour les propriétaires de sites, qui vont souffrir d'un risque plus élevé de harcèlement, d'intimidation et de vol d'identité ». Il est vrai que, malgré les gardes fous prévus par l'ICANN, la plupart des informations fournies pour l'enregistrement d'un nom de domaine sont sensibles, tant IRL (In Real Life) que dans le monde virtuel. En appelant à s'opposer au texte, l'association entend faire réagir sur un recul de l'anonymat, qui affectera ceux qui portent des opinions impopulaires ou marginales mais aussi les lanceurs d'alerte et tous ceux susceptibles de dénoncer « la criminalité et la corruption ».

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.linformaticien.com/actualites/id/37199/whois-vos-informations-personnelles-bientot-publiques.aspx>

Par Guillaume Périsat