Les nouvelles technologies guideront bientôt nos virées shopping | Le Net Expert Informatique

	Les nouvelles technologies guideront bientôt nos virées shopping

Cintres et miroirs intelligents, clés et porte-monnaie virtuels… Les objets connectés envahissent les centres commerciaux. Ils sont de plus en plus plébiscités par les Français.

Les centres commerciaux, futurs temples ultra connectés? C'est apparemment ce que souhaiteraient les Français. Une enquête* menée par Unibail-Rodamco, le géant de l'immobilier commercial spécialisé dans les centres commerciaux des grandes villes, analyse les comportements des Français en matière de shopping et identifie les tendances de demain. À chaque étape du shopping son innovation. Près de 65% des clients souhaiteraient voir le prix, la taille ou la composition du vêtement s'afficher automatiquement sur le cintre. Plus facile, le shopping.
Une majorité de clients voudrait avoir des conseils personnalisés de la part des vendeurs. Et plus surprenant – à l'heure où l'adoption de la loi sur le renseignement a tant fait polémique – presque la moitié des sondés désire recevoir chez eux des produits suggérés par un service qui analyse leurs données personnelles. L'autre enjeu, très attendu: celui de gagner du temps. Les «serial shoppers» sondés sont 62% à être favorables à l'essayage virtuel en magasin. Et pour cela, l'enseigne Uniqlo a trouvé le filon: le «magic mirror» est relié à une tablette et permet de modifier le coloris du vêtement porté sans avoir à le changer. Dans le même ton, plus de la moitié des Français pensent que les porte-monnaie virtuels seront démocratisés dans les années à venir (Paypal, paiement sans contact etc.). «Aujourd'hui, une clé virtuelle permet même de se faire livrer ses achats dans le coffre de sa voiture», raconte Clémentine Piaza, directrice marketing d'Unibail-Rodamco. Appelée «volvo on call», cette clé sollicitée par 55 % des sondés permet d'ouvrir la voiture uniquement pendant le laps de temps défini avec l'acheteur pour charger le coffre.

Expérience collective
Le centre commercial demeure le lieu de shopping privilégié des Français, et plus de 70% des hommes y vont accompagnés, selon l'étude. «L'époque du consommateur individualiste et narcissique est désormais révolue car il est maintenant à la recherche, à travers le shopping, d'une expérience durant laquelle il retrouve un moment commun, un engagement,une appartenance à un groupe de référence», analyse Stéphane Hugon, Docteur en sociologie, chercheur au Centre d'Etudes sur l'Actuel et le Quotidien.
Service de géolocalisation pour retrouver ses amis présents dans le centre, échanges de photos facilités ou café conçu pour partager une expertise et des conseils à l'image de DimensionAlley à Berlin, tout est pensé pour répondre à «un besoin de connexion permanent». Deux tiers des sondés rêvent enfin d'espaces plus aérés intégrant verdure et silence, mais aussi d'espaces vivants et animés. D'une sorte de ville nouvelle à la pointe de la technologie. À l'image du nouveau centre SuperPier à Manhattan, qui ouvrira ses portes cet été.
*La 3ème édition de L'Observatoire du Shopping Unibail-Rodamco a été menée auprès de 2006 individus constituant un échantillon représentatif de la population française âgée de 16 à 70 ans. Le recueil des données a été réalisé du 16 au 23 mars 2015, via l'Access Panel Online d'Ipsos, utilisant la méthode des quotas (âge, profession de la personne interrogée, région et catégorie d'agglomération).

Source : http://www.lefigaro.fr/conso/2015/07/11/05007-20150711ARTFIG00007-les-nouvelles-technologies-guideront-bientot-nos-virees-shopping.php

Les 10 outils les plus incroyables utilisés par la NSA pour nous espionner | Le Net Expert Informatique

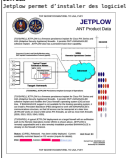
Les 10 outils les plus incroyables utilisés par la NSA pour nous espionner

Le journal allemand Der Spiegel a lancé des révélations chocs sur le cyberespionnage à partir de documents confidentiels partagés par l'ancien consultant de la NSA Edward Snowden. Voici un palmarès des outils les plus fous utilisés par la National Security Agency pour nous espionner. Il semblerait que pour chaque porte verrouillée par les fournisseurs d'équipements réseaux, les produits informatiques et les télécoms, la NSA possède une clé. La liste complète de ces outils disponible ici.(http://leaksource.wordpress.com/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/)

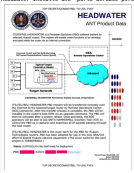
FEEDTHROUGH
Juniper Networks n'est ni plus ni moins que le 2e équipementier mondial de systèmes réseaux pour entreprises. Ses pare-feux Netscreen permettent de faire respecter la politique de sécurité d'un réseau informatique, définissant quels types de communication y sont autorisés. La NSA inflitre ce périmètre sécurisé grâce à Feedthrough.

DEITYBOUNCE
Deitybounce permet d'installer des logiciels malveillants de façon permanente, notamment sur les serveurs "PowerEdge" du fabricant mondial de PC Dell. La NSA implante son malware dans les "BIOSS", ces logiciels sur la carte mère d'un ordinateur qui sont les premiers éléments installés au démarrage de l'appareil. Le PC ou serveur infecté semble fonctionner normalement, et même s'il est nettoyé, et son contenu entièrement effacé, les logiciels espions de la NSA restent logés de façon invisible. Dell a répondu à cette révélation (http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2013/12/30/comment-on-der-spiegel-article-regarding-nsa-tao-organization.aspx).

JETPLOW
Jetplow permet d'installer des logiciels espions permanents dans les pare-feux du géant mondial des réseaux informatiques Cisco. Il peut aussi "modifier le système d'opération des pare-feux de Cisco au démarrage". Une option de "porte dérobée permanente" permet aussi "un accès complet". Cisco a répondu à cette révélation (http://blogs.cisco.com/news/comment-on-der-spiegel-articles-about-nsa-tao-organization).



HEADWATER
Headwater installe une "porte dérobée permanente" (Persistent Backdoor) sur certains routeurs du fabricant de matériel informatique chinois Huawei. Ces "implants" espions peuvent être installés à distance via internet.

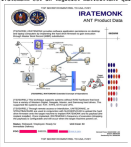


NIGHTSTAND
Nightstand est un appareil sans fil d'exploitation et d'insertion de données, "typiquement utilisé quand on ne peut accéder à une cible via une connexion internet." Il permet des attaques de loin, jusqu'à près de 13 kilomètres de distance de la cible.

PICASSO
D'apparence assez habituelle voire désuète, Picasso est un téléphone sans fil avec puce GSM (dont deux modèles de Samsung) qui permet de "collecter les données d'utilisateurs, des informations de géolocalisation et le son d'une pièce". Ces données peuvent être récupérées via un ordinateur portable ou bien par SMS "sans alerter la cible".

COTTONMOUTH-I
Pour le novice, cet outil ressemble à un port et câble USB inoffensifs. Mais à l'intérieur, se cache une carte mère qui fournit "un pont sans fil dans un réseau cible, ainsi que la possibilité d'introduire des logiciels « exploit » sur des ordinateurs portables ciblés." (Un "exploit" permet à un logiciel malveillant d'exploiter une faille de sécurité informatique dans un système d'exploitation ou un logiciel.) Autrement dit, la NSA peut introduire un cheval de Troie dans n'importe quel ordinateur.

IRATEMONK
Iratemonk est un logiciel malveillant qui infecte des ordinateurs portables et de bureau en attaquant le firmware de disques durs fabriqués par Western Digital, Seagate, Maxtor et Samsung, qui sont toutes à l'exception de la dernière, des entreprises américaines. Le firmware, ou microprogramme, concerne l'ensemble des instructions et des structures de données qui sont intégrées dans le materiel informatique.



TOTEGHOSTLY 2.0
Toteghostly 2.0 est un implant logiciel à destination du système d'exploitation Windows Mobile, qui permet d'extraire et d'installer des données à distance. La NSA peut ainsi accéder aux SMS, liste de contacts, messages vocaux, géolocalisation, fichiers audio et vidéo, etc. de l'appareil.

CANDYGRAM
Candygram est une "station GSM active", qui permet d'imiter le comportement d'une tour de téléphonie cellulaire et ainsi de repérer et monitorer des téléphones portables. Quand un appareil ciblé entre dans le périmètre de la station Candygram, le système envoie un SMS à l'extérieur du réseau à des téléphones "espions" préalablement enregistrés.

Tout cela sans compter Dropoutjeep qui permet à la NSA peut installer des logiciels espions sur les iPhone (http://www.usine-digitale.fr/article/la-nsa-peut-infiltrer-iphone-et-ipad-a-distance.N229076), et sur tous les appareils iOS et collecter ainsi des données sans que la "cible" s'en aperçoive.

Enfin, petit cadeau, dont Jean-Paul PINTE fait mention dans son blog le 6 juillet 2015, l'organigramme pratique des outils Internet de la NSA.

Source : http://www.usine-digitale.fr/article/les-10-outils-les-plus-incroyables-utilises-par-la-nsa-pour-nous-espionner.N229157
Par Nora Poggi

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

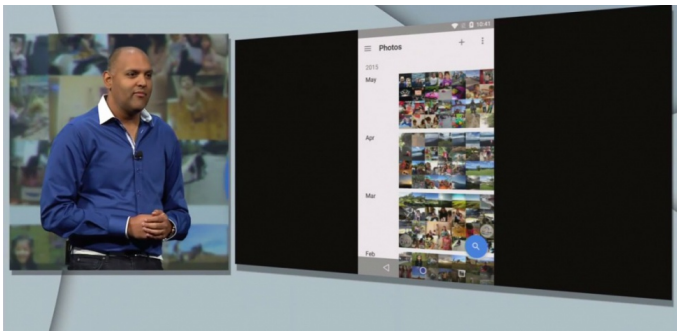
La Cnil interdit la géolocalisation du salarié en dehors du temps de travail

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.

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

Et maintenant Google veut vos photos. Toutes vos photos… | Le Net Expert Informatique



Ani Sabharwal, responsable de l'application Photos chez Google, lors de sa présentation au Google I/O le 29 mai 2015. Google

Et maintenant Google veut vos photos. Toutes vos photos…

Après les courriers électroniques, Google veut héberger toutes les photos des internautes. Et bien sûr, analyser leur contenu.

A peine quelques jours avant Apple, c'est Google qui a organisé sa grand-messe annuelle à l'attention des développeurs. L'occasion de se faire une idée des prochains développements sur lesquels mise le géant américain. Parmi eux, une application qui a de bonnes chances de faire mouche auprès du grand public : Google Photos. A première vue, rien de révolutionnaire, car il s'agit d'une application de stockage et de partage de ses photos. Mais avec le petit détail dont Google s'est fait une spécialité : le stockage illimité et gratuit. Et la taille du stockage, c'est ce qui avait assuré par le passé le succès de Gmail face aux messageries déjà implantées.

Un stockage gratuit et illimité

Pour la première fois, le grand public a donc une solution gratuite de sauvegarde de l'ensemble de ses photos et même de ses vidéos. Avec une limitation technique qui ne devrait pas poser de problème aux non-professionnels : la qualité des photos est limitée à 16 mégapixels et celle des vidéos à 1080p (limitation dont on peut se défaire pour 10 dollars par mois et par teraoctet de données). L'interface est soignée, très épurée, dans la droite ligne des produits maison. On peut classer les photos, les retoucher, faire des montages. Google a aussi mis à disposition de chacun ses algorithmes de fouille d'image. Ainsi, toutes les photos sont analysées et l'application y reconnaît toute seule les visages ou des éléments comme par exemple de la nourriture. On peut théoriquement ainsi retrouver des photos en tapant des mots-clés dans le moteur de recherche sans jamais avoir « taggé » ses photos. Démonstration sur scène avec une recherche instantanée des photos après avoir dicté « tempête de neige à Toronto ». La recherche combine sans doute les éléments de neige sur l'image avec la géolocalisation de la ville.

La mort de Google+

Cette nouvelle application marque le premier signe du repositionnement de Google sur les réseaux sociaux. En effet, elle découle du début de démantèlement de Google+, qui n'a jamais su s'imposer face à Facebook. En séparant la partie photos de son réseau social, Google va essayer de reprendre du terrain sur les images. D'autant que l'application n'existe pas que sur le web ou les appareils Android : elle est aussi disponible sur iOS (le système d'exploitation d'Apple), ce qui en fait un grand concurrent du stockage des photos sur le cloud d'Apple, qui lui est facturé au prix fort : de 0,99 € par mois pour 20 Go à 19,99 € pour 1 To. Avec ce nouveau service, Google semble bien armé pour réussir ce qu'il a fait avec Gmail : garder l'internaute dans son propre univers en hébergeant ses données personnelles, afin de pouvoir par la suite se rémunérer avec la publicité. En sachant en plus cette fois tout ce qu'il y a dans ses photos et où et quand elles ont été prises.

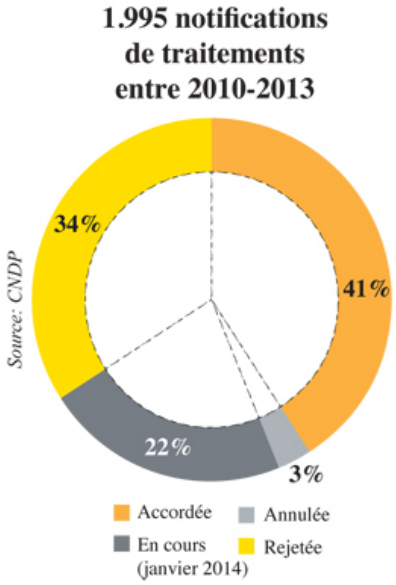
La conférence est à revoir en intégralité ici :

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

Source : http://www.sciencesetavenir.fr/high-tech/20150529.OBS9810/et-maintenant-google-veut-vos-photos-toutes-vos-photos.html?cm_mmc=EMV-_-SEA-_-20150531_NLSEAACTU-_-et-maintenant-google-veut-vos-photos-toutes-vos-photos##xtor=EPR-6-ActuSciences17h-20150531

Attention à l'usage abusif de

la géolocalisation | Denis JACOPINI



Attention à l’usage abusif de la géolocalisation

Pour les besoins de leurs activités, certains opérateurs de transport et logistique surtout utilisent la géolocalisation. Technologie qui permet de pister un véhicule de service par exemple (voir encadré). Malgré la légitimité de leur prétention, ses utilisateurs sont-ils pour autant en règle avec la loi?

Le traitement de données peut porter atteinte à la vie privée. D'où l'interdiction par exemple de suivre les déplacements d'un salarié hors service. La réglementation en vigueur prévoit des garde-fous: finalité du traitement, nature des données collectées, durée de leur conservation, droits des personnes concernées, consentement des salariés… Une formalité de grande importance à respecter. L'entreprise doit notifier le traitement à la «Commission nationale de contrôle de protection des données à caractère personnel (#CNDP), en France, la Commission Nationale Informatique et Libertés (CNIL). Une demande de déclaration-type est mise à leur disposition. Une demande d'autorisation (et non de déclaration) distincte s'impose à la société qui procède à l'interconnexion ou au recoupement avec d'autres fichiers dont les principales finalités sont différentes. L'employeur doit donc se conformer à toutes ces règles.

Par quoi doit-il commencer?

La finalité du traitement impose que le dispositif de géolocalisation ne soit installé que dans un véhicule à usage professionnel. Une société est en droit de rationaliser la gestion de son parc automobile, d'assurer le secours de son personnel en cas d'incident ou d'accident, facturer une prestation au juste prix (kilométrage, consommation, temps…).
Garantir la sécurité des marchandises et des véhicules est également un motif légitime. L'évaluation du rendement des conducteurs est aussi envisageable. Ce cas-là est verrouillé par l'autorité de contrôle (CNDP ou CNIL): la géolocalisation n'est justifiable que «lorsqu'il n'y pas d'autres moyens» pour jauger la productivité d'un salarié. Cette exception ouvre la porte au débat: un syndicat qui, tout en cautionnant l'installation du système, s'oppose à sa prise en compte dans le rendement des salariés.

Que valent aussi les données emmagasinées et utilisées dans une procédure de licenciement pour faute grave?

La géolocalisation «ne doit être activée que si le véhicule est utilisé à des fins professionnelles», précise la CNDP dans sa Délibération n°17-2014. Voilà qui réduit sensiblement la marge d'exploitation de ce système par un employeur.
Celui-ci doit aussi être particulièrement prudent sur la nature des données collectées. Elles sont réparties en deux rubriques. Nom, prénom, coordonnées professionnelles, sont des informations liées directement au salarié. Il y a ensuite des données qui renseignent plutôt sur le véhicule suivi: numéro de plaque d'immatriculation, position géographique, kilométrage parcouru, horaire et durée d'utilisation du véhicule et de conduite, nombre d'arrêts et la vitesse moyenne de circulation. La durée de conservation est limitée à un an. Au-delà, l'exploitation de ces informations serait illégale. Annulant ainsi leur portée dans une procédure disciplinaire ou judiciaire par respect notamment du principe de la loyauté de la preuve.
Le droit d'information pèse dans la mise en place du système de géolocalisation. Au même titre que l'utilisation des caméras de surveillance, une notice s'impose pour informer les salariés: nom du responsable du traitement, nature et destinataires des données, finalité de la collecte…
A moins de justifier «l'existence d'une dérogation», le consentement «libre et éclairé» des conducteurs est indispensable. Exemple: l'insertion d'une clause «géo-localisation» dans le contrat de travail des futures recrues. Toutefois, l'information préalable des instances représentatives des employés demeure la règle. Une obligation à respecter avant l'installation du dispositif de géolocalisation. Seul le gestionnaire du parc automobile et le service ressources humaines, éventuellement, peuvent accéder aux données. Les responsables de traitement doivent donc être identifiables au sein de l'entreprise et sont, en cas de contrôle, les interlocuteurs des agents assermentés de la CNDP. Ils ont pour charge de veiller à la sécurité et à la confidentialité des données. La divulgation d'une information ou son exploitation abusive engagent la responsabilité civile, voire pénale, du dirigeant et des responsables de traitement.

Un droit à double tranchant

La géolocalisation permet d'identifier la position d'un objet ou d'une personne en ayant recours aux bornes wifi, antenne GSM et position de constellation satellitaire. L'une de ses utilisations les plus courantes est le suivi des véhicules de service: optimiser les déplacements, le temps, la consommation de carburant.

«Consciente de son utilité», la commission nationale de contrôle de protection des données à caractères personnel (CNDP) définit des règles aux responsables de traitement afin que le dispositif de géolocalisation soit conforme avec la loi 09-08 protégeant les données privées. Toute infraction à la réglementation expose son auteur à de lourdes amendes, voire dans certains cas à l'emprisonnement.

Ces informations concernent le Maroc. Un équivalent pour la France Existe.
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.leconomiste.com/article/971816-attention-l-usage-abusif-de-la-geolocalisation
Par Faical FADOUNI

L’employeur face au droit d’accès du salarié à ses données informatiques | Le Net Expert Informatique

L’employeur face au droit d’accès du salarié à ses données informatiques

Pour Isabelle Renard, docteur ingénieur et avocate au barreau de Paris, la loi Informatique et libertés encadre encore de manière floue les relations employeurs/employés, notamment dans le cadre de l'accès au salarié à ses traces « informatiques ». Elle recommande aux entreprises d'encadrer de façon explicite et précise dans leur charte informatique les modalités de ce droit d'accès, pour éviter les demandes abusives de la part de leurs employés.

La loi Informatique et libertés prévoit que toute personne dont les données personnelles sont traitées peut demander au responsable de traitement d'accéder à celles-ci, dans des conditions qui sont précisées par l'article 39 du texte.
Aux termes de ces dispositions, chacun peut obtenir l'ensemble des renseignements qui caractérisent le traitement dont ses données font l'objet : quelles sont les données traitées, dans quel but, à qui sont-elles transmises, le responsable s'appuie-t-il sur ces informations pour prendre des décisions personnelles à l'égard de la personne concernée ?
Le responsable du traitement des data est tenu de répondre à ces interrogations, sauf si celles-ci procèdent d'un abus manifeste, par leur nombre ou leur répétition trop systématique.
Ces dispositions sont entièrement applicables aux relations entre salariés et employeurs qui, avec les nouvelles technologies, sont en possession de données personnelles de plus en plus nombreuses concernant leurs employés : données de connexion Internet, gestion centralisée des compétences, données des badgeuses, géolocalisation, enregistrements vidéos et vocaux…

UNE FICHE PRATIQUE DE LA CNIL
Les données des employés doivent être collectées licitement, ce qui suppose que les employeurs aient déclaré à la Commission nationale de l'informatique et des libertés (Cnil) les traitements afférents, selon la procédure applicable (déclaration simplifiée, normale, ou demande d'autorisation), selon qu'il existe – ou non – un correspondant informatique et libertés dans l'entreprise. En cas de non déclaration ou de déclaration partielle par l'employeur d'un fichier, les données recueillies ne peuvent pas être opposées au salarié pour fonder une procédure disciplinaire. Ce principe posé par le Cour de cassation est rappelé de façon constante par la jurisprudence.
Mais ce n'est pas tout. Encore faut-il que l'employeur soit en mesure de répondre aux demandes d'accès à leurs données exercées par les salariés. La Cnil, dans la fiche pratique numéro 3 de son guide « pour les employeurs et les salariés », donne une liste des informations auxquelles le salarié a le droit d'accéder, sur simple demande :
• recrutement
• historique de carrière
• rémunération
• évaluation des compétences professionnelles (entretiens d'évaluation, notations)
• dossier disciplinaire
De façon générale, le salarié doit pouvoir accéder à l'ensemble des données de gestion de ressources humaines le concernant, dès lors que celles-ci ont servi de base à une décision à son égard. Ce critère manque singulièrement de clarté, et semble ne concerner que les données de ressources humaines.
S'agissant des traces informatiques, la Cnil ne met aucune condition à leur droit d'accès par le salarié. Par exemple, pour les données de géolocalisation, elle a prononcé une sanction de 10 000 euros à l'encontre de la société Nord Picardie, qui a refusé de transmettre à un employé une copie de ses données de géolocalisation, dont il avait besoin pour prouver qu'un accident de la circulation dont il avait été victime avait un caractère professionnel. De la même façon, l'employeur est tenu de mettre à disposition d'un salarié en faisant la demande ses données de vidéosurveillance, ses écoutes téléphoniques ou ses données de navigation web.

UNE CHARTE INFORMATIQUE EXPLICITE
Confrontés à de telles requêtes l'employeur, même de bonne foi, a parfois du mal à savoir comment se positionner, surtout lorsque lesdites requêtes sont exercées par certains salariés uniquement par principe, pour obliger l'employeur à se plier à une exigence qu'ils estiment être de droit, et alors même que la fourniture de ces informations hors contexte peut se heurter à de réelles difficultés pratiques. Ne reste alors à l'employeur qu'à sortir le joker de la demande « manifestement abusive », et pour cela, il faut caractériser l'abus, ce qui n'est pas simple.
Le « droit d'accès » prévu de façon générale par la loi Informatique et libertés reste un sujet mal encadré dans les relations employeurs/employés, surtout s'agissant de l'accès au salarié à ses traces « informatiques », dont il est en tout état de cause informé de la collecte dès lors que celle-ci est clairement mentionnée dans la charte informatique. Le point n'est pas plus traité dans le projet de règlement européen sur la protection des données personnelles.
Faute d'attendre une amélioration des textes ou un positionnement de la Cnil, nous pensons que la meilleure façon pour les employeurs de se prévaloir de demandes abusives est d'encadrer de façon explicite et précise dans les chartes informatiques les modalités du droit d'accès, pour chaque type de trace « numérique », au lieu des dispositions génériques et floues qu'on y voit actuellement.

Source : http://www.usine-digitale.fr/article/l-employeur-face-au-droit-d-acces-du-salarie-a-ses-donnees-informatiques.N330908
Par Isabelle Renard, docteur ingénieur et avocate au barreau de Paris

Enjeux et défis du web profond | Le Net Expert Informatique

Le web profond (Deep Web) désigne le sous-ensemble d'internet qui n'est pas indexé ou mal indexé par les grands moteurs de recherche comme Google, Yahoo ou Bing,…On sait que cet ensemble de données reste difficilement mesurable mais qu'il occupe un espace très supérieur à celui de l'ensemble des sites web bien indexés par les moteurs classiques. Certaines études avancent un ratio de 80% de Deep Web contre 20% de web de surface à l'image de la partie immergée d'un iceberg…

Profond comme le web

Le contenu du deep web demeure hétérogène. On y trouve de grandes bases de données, des bibliothèques volumineuses non indexées par les moteurs en raison de leur tailles, des pages éphémères, mal construites, à très faible trafic ou volontairement rendues inaccessibles par leurs créateurs aux moteurs traditionnels.
D'après une étude récente de la Darpa, l'agence américaine en charge des projets de défense, plus de 60 millions de pages à vocation criminelle ont été publiées depuis deux ans dans les profondeurs du web. Les moteurs de recherche classiques, Google en tête, utilisent des algorithmes d'indexation dérivés du puissant Pagerank qui s'appuient sur une mesure de popularité du site ou de la page.
Cette approche qui a fait le succès de Google va de fait exclure les pages à faible trafic, éphémères ou furtives. Ce sont précisément ces pages qui sont utilisées par les acteurs de la cybercriminalité pour diffuser de l'information tout en restant sous les radars des grands moteurs. Lorsque cette information concerne une activité criminelle, c'est dans le Dark Web qu'elle sera dissimulée et rendue accessible aux seuls clients potentiels via des outils d'anonymisation spécialisés comme Tor. Le web profond réunit donc de la donnée légitime, souvent de haute qualité lorsqu'il s'agit de bases de données scientifiques volumineuses peu ou mal indexées par les moteurs.
Il réunit de la donnée sécurisée accessible seulement par mot de passe mais aussi de la donnée clandestine issue de trafics et d'activités criminelles. Cet ensemble informationnel hétérogène intéresse depuis longtemps les grands acteurs du numérique, chacun avec une motivation spécifique. L'accès au web profond constitue un élément stratégique du dispositif global de lutte contre la cybercriminalité qui reste l'une des grandes priorités de l'administration américaine. Les efforts pour obtenir des capacités de lecture du web profond se sont concrétisés avec le développement en 2014 du moteur de recherche Memex tout droit sorti des laboratoires de la Darpa.

Memex, le moteur Darpa

Dans son communiqué officiel publié le 9 février 2014 [1], l'agence Darpa décrit Memex comme « le moteur qui révolutionne la découverte, l'organisation et la présentation des résultats de recherche en ligne. Le programme Memex imagine un nouveau paradigme, où il est possible d'organiser rapidement et intelligemment un sous-ensemble de l'internet adapté à l'intérêt d'une personne ».

Le moteur est construit autour de trois axes fonctionnels:
1. l'indexation de domaines spécifiques,
2. la recherche de domaines spécifiques
3. la mise en relation de deux premiers axes

Après plus d'un an d'utilisation en phase de test par les forces de l'ordre américaines, Memex a permis de démanteler un réseau de trafiquants d'êtres humains. Durant la finale du Super Bowl, Memex a servi pour détecter les pages associées à des offres de prostitution. Ses outils d'analyse et de visualisation captent les données invisibles issues du web profond puis tracent la graphe des relations liant ces données. De telles fonctionnalités s'avèrent très efficaces pour cartographier des réseaux clandestins de prostitution en ligne.

D'après les récents communiqués de la Darpa, Memex ne traite pour l'instant que les pages publiques du web profond et ne doit donc pas être associé aux divers outils de surveillance intrusifs utilisés par la NSA. A terme, Memex devrait offrir des fonctionnalités de crawling du Dark Web intégrant les spécificités cryptographiques du système Tor. On peut raisonnablement imaginer que ces fonctions stratégiques faisaient bien partie du cahier des charges initial du projet Memex dont le budget est estimé entre 15 et 20 millions de dollars… La Darpa n'est évidemment pas seule dans la course pour l'exploration du web profond. Google a parfaitement mesuré l'intérêt informationnel que représentent les pages non indexées par son moteur et développe de nouveaux algorithmes spécifiquement adaptés aux profondeurs du web.

Google et le défi des profondeurs

Le web profond contient des informations provenant de formulaires et de zones numériques que les administrateurs de sites souhaitent maintenir privés, hors diffusion et hors référencement. Ces données, souvent très structurées, intéressent les ingénieurs de Google qui cherchent aujourd'hui à y avoir accès de manière détournée. Pour autant, l'extraction des données du web profond demeure un problème algorithmiquement difficile et les récentes publications scientifiques des équipes de Google confirment bien cette complexité. L'Université de Cornell a diffusé un article remarquable décrivant une infrastructure de lecture et de copie de contenus extraits du web profond [2],[3].

L'extraction des données s'effectue selon plusieurs niveaux de crawling destinés à écarter les contenus redondants ou trop similaires à des résultats déjà renvoyés. Des mesures de similarités de contenus sont utilisées selon les URL ciblées pour filtrer et hiérarchiser les données extraites. Le système présenté dans l'article est capable de traiter un grand nombre de requêtes sur des bases de données non adressées par le moteur de recherche classique de Google [4].

A moyen terme, les efforts de Google permettront sans aucun doute de référencer l'ensemble du web profond publiquement accessible. Le niveau de résolution d'une requête sera fixé par l'utilisateur qui définira lui même la profondeur de sa recherche. Seuls les contenus privés cryptés ou accessibles à partir d'une identification par mot de passe demeureront (en théorie) inaccessibles à ce type de moteurs profonds.

Vers une guerre des moteurs?

Les grandes nations technologiques ont pris en compte depuis longtemps les enjeux stratégiques de l'indexation des contenus numériques. Peu bruyante, une « guerre » des moteurs de recherche a bien lieu aujourd'hui, épousant scrupuleusement les contours des conflits et les concurrences de souverainetés nationales. La Chine avec son moteur Baidu a su construire très tôt son indépendance informationnelle face au géant américain.

Aujourd'hui, plus de 500 millions d'internautes utilisent quotidiennement Baidu à partir d'une centaine de pays. La Russie utilise massivement le moteur de recherche Yandex qui ne laisse que peu de place à Google sur le secteur du référencement intérieur russe puisqu'il détient plus de 60% des parts du marché national. En 2014, Vladimir Poutine a souhaité que son pays développe un second moteur de recherche exclusivement contrôlé par des capitaux russes et sans aucune influence extérieure. Plus récemment, en février 2015, le groupe Yandex a déposé une plainte contre Google en Russie pour abus de position dominante sur les smartphones Android. Yandex reproche en effet à Google de bloquer l'installation de ses applications de moteur de recherche sur les smartphones fonctionnant sous Android. Les constructeurs sont contraints aujourd'hui à pré-installer sur leurs machines les Google Apps et à utiliser Google comme moteur par défaut sous Android…

Le moteur face aux mégadonnées

La course à l'indexation des contenus du web profond apparaît comme l'une des composantes stratégiques de la guerre des moteurs. Si la géopolitique des données impose désormais aux nations de définir des politiques claires de stockage et de préservation des données numériques, elle commande également une vision à long terme de l'adressage des contenus. La production mondiale de données dépassera en 2020 les 40 Zo (un zettaoctet est égal à dix puissance vingt et un octets). L'évolution de cette production est exponentielle: 90% des données actuelles ont été produites durant les deux dernières années. Les objets connectés, la géolocalisation, l'émergence des villes intelligentes connectées et de l'information ubiquitaire contribuent au déluge de données numériques. La collecte et l'exploitation des mégadonnées (le terme officiel français à utiliser pour big data) induiront le développement de moteurs polyvalents capables d'indexer toutes les bases de données publiques quelle que soient leurs tailles et leurs contenus.

Le moteur de recherche doit être considéré aujourd'hui comme une infrastructure de puissance stratégique au service des nations technologiques. Qu'attend l'Europe pour développer le sien?

_____

[1] La présentation du moteur Memex par l'agence Darpa
http://www.darpa.mil/newsevents/releases/2014/02/09.aspx
[2] « Google's Deep-Web Crawl » – publication de l'Université Cornell
http://www.cs.cornell.edu/~lucja/publications/i03.pdf
[3] « Crawling Deep Web Entity Pages » – publication de recherche, Google
http://pages.cs.wisc.edu/~heyeye/paper/Entity-crawl.pdf
[4] « How Google May index Deep Web Entities »
http://www.seobythesea.com/2015/04/how-google-may-index-deep-web-entities/

Source : http://www.huffingtonpost.fr/thierry-berthier/enjeux-et-defis-deep-web_b_7219384.html
Par Thierry Berthier

Survols illégaux de drones : le SGDSN fait le point | Le Net Expert Informatique

Un drone civil grand public tel que ceux qui ont pu être utilisés pour réaliser des survols illégaux. Ici, un drone Bebop du constructeur Parrot ©TORU YAMANAKA / AFP

Survols illégaux de drones : le SGDSN fait le point

Le secrétariat général de la défense et de la sécurité nationale a présenté ce mercredi 6 mai 2015, un état des lieux dans la lutte contre les survols illégaux de drones, et a livré quelques pistes intéressantes
Depuis le 10 septembre 2014, 68 « incidents » ont été recensés en France chiffre le SGDSN, dont 29 au dessus de centres de production nucléaires, et 8 au dessus de sites militaires. A noter que pour le SGDSN, des survols multiples au cours d'une même journée ne constituent qu'un seul « incident ». L'écrasante majorité de ces survols ont eu lieu de nuit, puisque seulement 4 de ces « incidents » ont été constatés de jour. Ce qui explique aussi que de nombreux témoignages soient soumis à caution. « On nous a signalé de tout, aussi bien des machines multirotor à décollage vertical que des ailes volantes », témoigne le colonel Julien Sabéné, à la direction protection et sécurité de l'État. Ces survols ont donné lieu à « quelques interpellations » nous a précisé le SGDSN sans donner de chiffre exact ni plus de précision, les enquêtes étant toujours en cours.

Le SGDSN a par ailleurs rappelé que si des survols illégaux avaient eu lieu dans de nombreux autres pays d'Europe (Belgique, Suisse, Royaume Uni, Allemagne…) ainsi qu'aux Etats-Unis (qui investissent « plusieurs milliards de dollars » pour développer des technologies anti drones civils) et au Japon, les survols massifs au dessus des villes ou des centrales nucléaires constituent en revanche une spécificité française.

Certains de ces survols paraissaient bien coordonnés. Toutefois, le SGDSN affirme que cette coordination n'est pas forcément le fait d'une organisation qui superviserait les manœuvres. Est évoquée à demi-mot la piste du défi que se lanceraient des pilotes de drones, de plus en plus nombreux, via Internet. Actuellement, il y aurait en France un parc d'environ 200.000 drones civils, et environ 1300 entreprises privées exploitant pour un usage professionnels 2000 à 2500 machines privées, estime le SGDSN.

À la recherche de « briques technologiques »
Outre l'appel à projet lancé auprès de l'Agence nationale pour la recherche (ANR) pour développer des solutions techniques capables de répondre à ce qui pourrait ressembler à une menace, le SGDSN a également invité en mars 2015 une vingtaine d'entreprises françaises à participer à une expérimentation. « L'objectif était de dresser l'état de l'art et de repérer d'éventuelles briques technologiques intéressantes », explique François Murgadella, responsable du développement des technologies de sécurité pour compte du SGDSN. Certaines de ces technologies ont démontré qu'il était possible de repérer un drone à une distance de 4km, de l'identifier à 2km, et de le neutraliser à 350m. Toutefois, la partie neutralisation est celle qui a encore le plus besoin de maturation.
Les éléments techniques ainsi repérés pourront donc venir compléter les études menées dans le cadre des deux projets retenus suite à l'appel à projet de recherche et de développement sur la protection des zones sensibles vis-à-vis du survol des drones aériens de l'ANR.

Le SGDSN a par ailleurs précisé qu'un nouvel appel à projet similaire pourrait être lancé en 2016, au niveau européen cette fois, « avec une enveloppe plus importante » précise François Murgadella (l'appel à projet de l'ANR portait sur une enveloppe de 1 millions d'euros de financement public).

LÉGISLATION
Enfin, outre les aspects techniques, le SGDSN a rappelé qu'elle envisageait de faire évoluer les règlementations en cours. Pas tellement vers un durcissement des lois mais plutôt vers une meilleure information vis-à-vis des nouveaux pilotes (par le biais notamment de formations en ligne), d'enregistrement des machines (immatriculation par exemple) ou via des dispositifs « gagnant – gagnant » permettant par exemple aux pilotes de se déclarer avant d'effectuer un vol, d'équiper temporairement leurs machines d'une puce de géolocalisation, et de disposer alors d'un espace aérien dédié, de données techniques sur le vol qu'ils réalisent, ainsi que d'outils permettant de retrouver leurs machines en cas de crash.

Source : http://www.sciencesetavenir.fr/high-tech/20150506.OBS8481/survols-illegaux-de-drones-la-sgdsn-fait-le-point.html
Par Erwan Lecomte

Les 5 dangers du projet de

loi sur le renseignement | Denis JACOPINI

	**Les 5 dangers du projet de loi sur le renseignement**

Dernière ligne droite pour le projet de loi sur le renseignement. Le vote solennel du texte est prévu ce mardi 5 mai à l'Assemblée, malgré une mobilisation des opposants, lundi soir au Trocadéro, à Paris.
Que dit le texte ? Au fil des débats, les députés ont fait évoluer le projet de loi. « Il a été considérablement enrichi », estime son rapporteur, Jean-Jacques Urvoas (PS), dans une note envoyée aux députés dont « l'Obs » a eu connaissance. Au total, 260 amendements ont été adoptés. Cela répond en partie aux demandes des adversaires du texte, mais ne lève pas toutes les inquiétudes, loin de là.

Ce que l'Assemblée a modifié :
Une commission de contrôle renforcée
Est surtout renforcé « la composition, l'indépendance et les pouvoirs de la [nouvelle] Commission nationale de contrôle des techniques de renseignements » (CNCTR). Celle-ci remplacera l'actuelle Commission nationale des interceptions de sécurité (CNCIS) et, comme réclamé dans « l'Obs » par son actuel président, cette nouvelle instance disposera d'un « accès aux locaux des services, aux dispositifs de traçabilité, aux opérations de transcription, d'une saisine élargie du Conseil d'Etat ». De plus, les renseignements collectés seront bien centralisés par le Groupement interministériel de contrôle (GIC), que « l'Obs » a pu visiter en exclusivité.

Des professions moins exposées
Le texte exclut désormais certaines professions de la procédure d'urgence. Pour les magistrats, les avocats, les journalistes et les parlementaires, les écoutes ne peuvent être mises en œuvre que sur autorisation du Premier ministre, après avis de la commission. (Art. L. 821-7)

Un statut de lanceur d'alerte
De même, un « statut de lanceur d'alerte a été créé afin d'apporter une protection juridique à tout agent souhaitant révéler des illégalités commises ». N'est en revanche pas précisé si ce statut pourra être étendu à tous ceux qui révèlent des illégalités, à la manière d'Edward Snowden sur la NSA.

Les hackers plus fortement sanctionnés
Les députés ont également profité du texte pour renforcer l'arsenal de sanctions contre les hackers. Dans le sillon de la cyberattaque contre TV5 Monde, ils ont décidé de doubler les sanctions pécuniaires pour tout piratage (actuellement puni au maximum de 75.000 euros), voire de les tripler s'il s'agit d'un service de l'Etat.

Un fichier des personnes mises en cause pour terrorisme
Le gouvernement a également profité de cette loi pour créer un nouveau fichier (FIJAIT) qui recensera les noms et adresses de toutes les personnes condamnées ou mises en examen pour terrorisme.

Malgré des améliorations notables du texte, certains points continuent de poser problème.

1 – Le Premier ministre, seul maître à bord
La loi dote les six services de renseignement français de nombreux moyens supplémentaires pour enquêter, et la plupart n'auront plus besoin de l'aval d'un juge. En effet, le Premier ministre se positionne comme seul décisionnaire.
Les autorisations sont délivrées, après avis de la CNCTR, par le Premier ministre », pointe le texte.
Surtout que le Premier ministre pourra passer outre l'avis de la CNCTR, mais devra alors motiver sa décision (et risquer une saisine du Conseil d'Etat). Et tout ceci s'applique, sauf « en cas d'urgence absolue »…

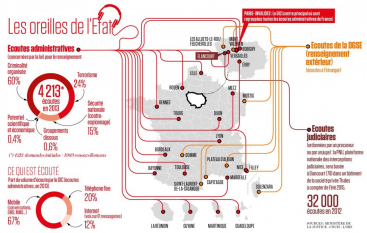
2 – Des données conservées longtemps
Afin de surveiller une personne, le projet de loi prévoit de nombreuses interceptions à distance (e-mails, conversations téléphoniques, SMS…) mais aussi la pose de micros et caméras dans des lieux ou des véhicules. Le texte prévoit que l'ensemble des renseignements ainsi collectés seront détruits au terme de certaines durées :
• 30 jours pour les correspondances,
• 90 jours pour les sonorisations, les géolocalisations et les images vidéo,
• 5 ans pour les données de connexion, aussi appelées métadonnées (qui donnent le détail de qui écrit un e-mail à qui, à quelle heure, etc.).
Et, en cas de cryptage des données, ces délais ne s'appliquent qu' »à compter de leur déchiffrement ».

3 – Eviter de croiser la route d'un suspect
Le projet de loi prévoit que les mesures de surveillance seront utilisées à la fois pour les suspects, mais aussi pour les « personnes appartenant à [son] entourage » s'il « existe des raisons sérieuses de croire [qu'elles ont] joué un rôle d'intermédiaire, volontaire ou non ». En somme, n'importe qui se trouvant au mauvais endroit, au mauvais moment, et ayant croisé une mauvaise route, pourra être mis sous surveillance.

Lors de la manifestation contre le projet de loi sur le renseignement, le 13 avril (CITIZENSIDE/ANTHONY DEPERRAZ/AFP)

4 – Tous suspects sur internet
Le projet de loi entend mettre à profit les opérateurs internet. Fournisseurs d'accès, moteurs de recherche, réseaux sociaux… Tous pourront fournir « en temps réel » les données techniques de connexion des internautes suspectés de terrorisme. Concrètement, il s'agit de pister une connexion (exprimée par une adresse IP) pour savoir quel site elle a visité, à quelle heure, si elle a envoyé un message Facebook à telle personne, si elle a tapé tel mot clef sur Google…
Le texte souhaite aussi contraindre les opérateurs internet à « mettre en œuvre sur leurs réseaux un dispositif destiné à détecter une menace terroriste sur la base de traitements automatisés ». Concrètement, les services de renseignement installeront une « boîte noire » dotée d'un algorithme qui passera au crible l'ensemble du trafic internet pour détecter automatiquement des internautes soupçonnés d'être des terroristes. A terme, cette boîte noire pourra être mise en place chez les fournisseurs d'accès à internet, mais aussi les Américains Google, Facebook, Apple ou Twitter.
L'ensemble du système surveille l'ensemble des internautes de manière anonyme pour détecter des « signaux faibles ». Et, en cas de suspicion, les opérateurs devront dénoncer la personne correspondant aux enquêteurs.
La CNCTR aura accès « au code source » de cette boîte noire afin de limiter la collecte des données aux seuls terroristes. Du moins, tant qu'un décret n'a pas étendu le champ d'action de ce dispositif qui s'apparente à « une surveillance de masse » inspirée par l'agence de renseignement américaine NSA.

5 – Surveiller les terroristes, mais pas seulement
Finalement, il convient de rappeler que, malgré les présentations du texte par François Hollande ou Manuel Valls, il ne s'agit pas d'une loi anti-terroriste, mais bien d'un texte sur le renseignement. Le projet prévoit sept finalités pour recourir aux diverses techniques de renseignement :
• l'indépendance nationale, l'intégrité du territoire et la défense nationale,
• les intérêts majeurs de la politique étrangère et la prévention de toute forme d'ingérence étrangère,
• les intérêts économiques, industriels et scientifiques majeurs de la France,
• la prévention du terrorisme,
• la prévention des atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la sécurité nationale ou de la reconstitution de groupements dissous,
• la prévention de la criminalité et de la délinquance organisées,
• la prévention de la prolifération des armes de destructions massives.
Pour rappel, en 2014, 60% des écoutes administratives visaient la criminalité organisée, 24% le terrorisme, 15% la sécurité nationale (contre-espionnage), 0,6% les groupements dissous, et 0,4% la protection du potentiel scientifique et économique. Depuis l'attaque meurtrière contre « Charlie Hebdo », la part dédiée au terrorisme est montée à 48%.



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

Note de Jean-Jacques Urvoas publié par NouvelObs.com

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

Source : http://tempsreel.nouvelobs.com/loi-renseignement/20150504.OBS8368/les-5-dangers-du-projet-de-loi-renseignement.html?cm_mmc=EMV-_-NO-_-20150505_NLNOACTU08H-_-les-5-dangers-du-projet-de-loi-renseignement##xtor=EPR-1-Actu8h-20150505
Par Boris Manenti

Multiplication des plaintes auprès de la CNIL | Le Net Expert Informatique

Multiplication des plaintes auprès de la CNIL

Refus de déréférencement par Google, vidéosurveillance excessive dans le milieu du travail, radiation des fichiers bancaires… Le nombre de plaintes déposées auprès de la Cnil augmente et concernent surtout les données personnelles visibles sur internet selon son 35è rapport d'activité 2014 publié le 18 avril.

Soucieux de protéger leur vie privée et surtout leurs données personnelles, les particuliers n'hésitent plus à saisir la Commission pour exercer leur droit d'opposition à figurer dans un fichier. 5 825 plaintes ont ainsi été recensées en 2014, un chiffre en augmentation de 3 % par rapport à 2013.
La Commission a par ailleurs traité plus de 2 200 plaintes motivées par un problème d'e-réputation : suppression de textes, photographies, vidéos, coordonnées, commentaires, faux profils en ligne ou encore à prévenir la réutilisation de données publiquement accessibles sur internet.
Depuis l'instauration d'un « droit à l'oubli » par la CJUE, 200 plaintes ont été déposées suite à des refus de déréférencement de la part des moteurs de recherche.
Parmi les exemples cités par la Cnil, on retrouve celui d'une internaute qui, après avoir tapé ses nom et prénom sur un moteur de recherche, a constaté qu'ils renvoient vers des sites pornographiques. Sa demande de déréférencement lui a été refusée dans un premier temps, avant d'être acceptée suite à son intervention.
Un autre sujet d'importance qui a retenu l'attention de la Commission est la géolocalisation ou la vidéosurveillance en milieu professionnel qui, à elle seule, a fait l'objet de 300 dossiers en 2014. Suivent les plaintes motivées par la contestation de l'inscription au fichier national des incidents de remboursement des crédits aux particuliers ou au fichier central des chèques et des retraits de cartes bancaires.
Outre internet, 16 % des plaintes concernent le commerce, et notamment les problèmes liés à la radiation de fichiers publicitaires, à la conservation des coordonnées bancaires, aux fichiers clients et à la possibilité de s'opposer à la réception des courriels publicitaires.

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

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

Source : http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/126183/Multiplication-des-plaintes-aupres-de-la-CNIL.aspx
Par Lionel Costes