Le chiffrement des smartphones Android incassable ?

	Le chiffrement des smartphones Android incassable ?

Un chercheur en sécurité décrit comment faire sauter la protection par chiffrement des données sur les smartphones Android équipés de puces Qualcomm.

Chiffrer l'ensemble de ses données sur un support de stockage est un bon moyen de les protéger en cas de perte ou vol du dit support. Néanmoins, il n'est pas infaillible. Particulièrement sur les smartphones Android équipés de processeurs Qualcomm. C'est ce que démontre le chercheur en sécurité Gal Beniamini. Dans un document très détaillé, il indique comment contourner les systèmes de protection. Et plus particulièrement, *« comment l'exécution du code TrustZone du noyau peut être utilisé pour briser efficacement le schéma de l'Encryption Full Disk d'Android »*, précise le chercheur.

Le Full Disk Encryption (FDE), la technique de chiffrement du disque d'Android, est proposé par Google depuis la version 5.0 de l'OS mobile. Il permet de générer des clés de chiffrement maître et esclave de 128 bits. La clé maître, également appelée DEK (pour Device Encryption Key) est protégée par chiffrement à partir du mot de passe, du code PIN ou du schéma de déverrouillage choisi par l'utilisateur. La DEK est stockée sur le smartphone (ou la tablette) dans un espace non chiffré de l'appareil, le *crypto footer*. Et c'est là que le problème survient. A cause d'une faille dans les processeurs de Qualcomm.

Utiliser une Trustlet

Pour comprendre pourquoi, il faut savoir que Android dispose, comme iOS, de mécanismes de temporisation et de blocage de l'appareil pour interdire les attaques par force brute (essais successifs de saisie des identifiants). Ces mécanismes sont liés au module KeyMaster qui s'exécute dans un environnement séparé de l'OS et considéré comme sécurisé, le Trusted Execution Environment (TEE). Le KeyMaster peut ainsi générer des clés de chiffrement sans les révéler au système d'exploitation. Une fois générées, ces clés sont à leur tour chiffrées et communiquées à l'OS. Quand ce dernier les sollicite, un bloc de données (le Blob, Binary Large OBject, un type de données qui permet l'intégration d'un pilote, souvent propriétaire, dans le code du noyau Linux) est fourni au KeyMaster sous forme d'une clé RSA de 2048 bits.

Mais le KeyMaster dépend de l'implémentation qu'en fait le fabricant sur son matériel. En l'occurrence, Qualcomm exploite bien le KeyMaster dans la TrustZone. Sauf que le TEE fourni par le constructeur, le QSEE (Qualcomm Secure ExecutionEnvironment), autorise des appliquettes (Trustlets) a s'exécuter dans cette zone sécurisée. Et, selon le chercheur, il est possible d'exécuter sa propre Trustlet dans la TrustZone en exploitant potentiellement une vulnérabilité Android. A partir de là, l'attaquant peut obtenir des privilèges administrateur et accéder au Blob qui contient les clés générées. Il ne reste alors plus qu'à lancer une attaque par force brute pour retrouver le code secret de l'utilisateur et disposer ainsi de la clé de déchiffrement du support de stockage.

Une correction difficile

Certes, la manœuvre n'est pas à la portée du premier venu. Et nécessite de disposer du terminal en main. Mais le déchiffrement d'un disque peut visiblement être exécuté par le fabricant des puces. Lequel peut avoir à se plier à une requête judiciaire comme on l'a vu avec Apple dans l'affaire de l'attentat de San Bernardino. Qui plus est, selon Qualcomm, le « bug » n'est pas facile à corriger. La correction demandera probablement une modification de l'architecture des processeurs. Lesquels équipent aujourd'hui une majorité de smartphones Android de la planète.

Néanmoins, le chercheur reste optimiste. *« J'espère qu'en jetant la lumière sur le sujet, cette recherche va motiver les équipementiers et Google à se réunir pour penser à une solution plus robuste pour le FDE*, écrit-il. *[…] Je crois qu'un effort concentré des deux côtés peut aider à rendre la prochaine génération d'appareils Android vraiment « inviolable ». »*

Article original de Christophe Lagane

Original de l'article mis en page : Le chiffrement des smartphones Android n'est pas incassable

---

Alerte : Une Backdoor destinée à voler les identifiants sur Mac OS X

(ESET)

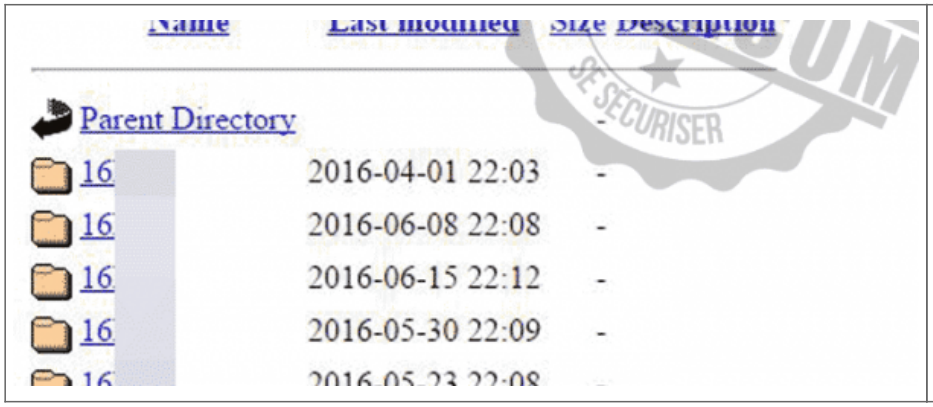
Alerte : Une Backdoor destinée à voler les identifiants sur Mac OS X (ESET)

Le malware Keydnap exfiltre les mots de passe et les clés stockés dans le gestionnaire de mot de passe « KeyChain » de Mac OS X et crée une porte dérobée permanente.

Les chercheurs ESET se sont penchés sur OSX/Keydnap, un cheval de Troie qui vole les mots de passe et les clés stockées dans le gestionnaire de mot de passe « keychain », en créant une porte dérobée permanente.
Bien que la façon dont les victimes se trouvent exposées à cette menace ne soit pas très clair, nous pensons qu'elle pourrait se propager via des pièces jointes contenues dans les spams, des téléchargements à partir de sites non sécurisés ou d'autres vecteurs.
Le code malveillant Keydnap est distribué sous forme de fichier .zip avec le fichier exécutable imitant l'icône Finder habituellement appliqué aux fichiers texte ou JPEG. Cela augmente la probabilité que le destinataire double-clique sur le fichier. Une fois démarré, une fenêtre de terminal s'ouvre et la charge utile malveillante est exécutée.
À ce stade, la porte dérobée est configurée et le malware débute la collecte et l'exfiltration des informations de base figurant sur la machine Mac attaqué. À la demande de son serveur C&C, Keydnap peut obtenir les privilèges administratifs en ouvrant la fenêtre dédiée d'OS X.
Si la victime saisit ses identifiants, la porte dérobée fonctionne alors comme un root, avec le contenu exfiltré du porte-clés de la victime.
Bien qu'il existe des mécanismes de sécurité multiples en place au sein d'OS X pour réduire l'impact des logiciels malveillants, il est possible de tromper l'utilisateur.
Tous les utilisateurs d'OS X doivent rester vigilants car nous ne savons toujours pas comment Keydnap est distribué, ni combien de victimes ont été touchées », rapporte Marc-Etienne M. Léveillé, Malware Researcher chez ESET.
Des détails supplémentaires sur Keydnap peuvent être trouvés dans notre article technique disponible sur WeLiveSecurity.com.

Réagissez à cet article
Source : ESET

Fuite de données colmatée pour l'Université de Bordeaux



Fuite de données colmatée pour l'Université de Bordeaux

Un problème informatique à l'université de Bordeaux donnait accès à plus de 15 000 dossiers d'étudiants. La CNIL est intervenue à la suite du protocole d'alerte de ZATAZ pour faire colmater une fuite de données que personne n'avait vue.

Tout a débuté voilà quelques semaines. Benjamin postule sur la plateforme APOFLUX de l'Université de Bordeaux. Rapidement, APOFLUX permet de déposer ses vœux pour rejoindre un cursus, une formation. Comme l'indique le site, APOFLUX est un outil de dépôt de vœux « ***Il ne s'agit en aucun cas de votre inscription administrative définitive à l'Université de Bordeaux***« . Bref, un espace ou les étudiants déposent des dizaines d'informations allant du simple au très sensible. « ***En cherchant une information sur mon dossier,*** m'expliquait alors Benjamin, ***je me suis rendu compte d'un – truc – plutôt moche***« . Et je trouve que le terme moche est très poli. Via un espace web non protégé baptisé « Dépôt », n'importe quel internaute avait accès à l'ensemble des dossiers des étudiants postulants. Chaque espace de stockage offrait à la lecture des curieux, de maladroits de la souris ou de violeurs d'intimité numérique, les relevés de notes, lettres de motivations, CV… ainsi qu'à l'ensemble des candidatures passées par APOFLUX. Le lien avait beau être en HTTPS, le S voulant dire que les connexions entre l'internaute et le serveur était chiffré, cela ne protégeait pas pour autant les informations sauvegardées.

Fuite de données colmatée, étudiant dans le silence

J'ai saisi la CNIL, qui au passage est d'une efficacité redoutable dès que je leur communique une alerte. Le problème a été colmaté en quelques heures. Pour le moment, l'université n'a pas contacté les étudiants concernés par cette fuite d'information. Espérons qu'aucun malveillant ne soit passé par là avant l'alerte de ZATAZ. Impossible de savoir depuis quand ces « portes ouvertes » étaient accessibles sur la toile.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Fuite de données colmatée pour l'Université de Bordeaux – ZATAZ

Le portable de Manuel Valls a-t-il été piraté par Israël ?

Le portable de Manuel Valls a-t-il été piraté par Israël ?

Lors de son déplacement en Israël, une délégation de Matignon a laissé ses portables sans surveillance pendant une réception officielle. Et a relevé des anomalies de fonctionnement sur certains terminaux ensuite, assure l'Express.

Manuel Valls s'est-il fait pirater son smartphone lors de son déplacement en Israël, fin mai dernier ? C'est la question que posent nos confrères de l'Express. Lors de son déplacement qui avait pour ambition de relancer le processus de paix avec la Palestine, le Premier ministre, qui se présente volontiers comme « l'ami d'Israël » et la délégation l'accompagnant ont été priés de laisser leurs téléphones portables à l'accueil avant d'être reçu en haut lieu. Demande à laquelle ils auraient accédé, laissant leurs terminaux sans surveillance pendant l'entretien.
Problème : quand ils ont récupéré leurs terminaux pourtant sécurisés, certains présentaient des « anomalies », selon l'Express. Des dysfonctionnements qui peuvent laisser suspecter une tentative d'intrusion de la part des services secrets israéliens. L'Express ne précise pas le ou les modèles des terminaux concernés par ces tentatives d'espionnage supposées.

Pas d'espionnage entre alliés. Sans blague ?
Depuis, les téléphones en question ont été remis à l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui mène l'enquête. Interrogée par nos confrères, celle-ci s'est toutefois refusée à tout commentaire. De son côté, Matignon reconnaît qu'un terminal est bien tombé en panne durant la visite du Premier ministre en Israël. Et indique à nos confrères qu'un allié n'espionne jamais ses amis. Défense de rire.
Rappelons que, pour les échanges les plus sensibles, les officiels français disposent de terminaux Teorem, fournis par Thales et habilités confidentiel-défense. Ceux-ci se révèlent toutefois peu pratiques d'usage, si bien que les ministres utilisent souvent des smartphones du commerce, durcis avec des technologies de sécurité complémentaires. Récemment, l'Elysée s'est ainsi équipé de smartphones Hoox, conçus par Bull. Ces machines, des smartphones Android bénéficiant d'une surcouche logicielle de sécurisation, sont vouées aux échanges de type « diffusion restreinte », un niveau de classification de l'information moins exigeant que le confidentiel-défense.
Article original de Reynald Fleychaux

Réagissez à cet article

Original de l’article mis en page : Le portable de Manuel Valls a-t-il été piraté par Israël ?

Un nouveau malware s’attaque aux Mac

Un nouveau malware s’attaque aux Mac

BitDefender a découvert Backdoor.MAC.Eleanor, un malware qui permet aux attaquants de prendre le contrôle des machines Apple sous Mac OS et de les piloter à travers le réseau d'anonymisation Tor.

Selon l'éditeur de sécurité, Eleanor est distribué sous forme d'un logiciel que l'on peut télécharger depuis des sites web légitimes dédiés à l'univers Apple. Une fois installé, l'agent malveillant affiche une interface de conversion de fichiers par drag&drop, service supposément légitime qui, en toute opacité, installe des composants sur le système. A partir de là, l'attaquant peut prendre le contrôle complet de la machine, y compris capturer des images depuis la webcam du portable. Comme Eleanor n'est pas certifiée Apple, les utilisateurs sous El Capitan, la dernière version d'OS X verront s'afficher un message d'alerte de sécurité lors de l'installation de l'application infectieuse. Une barrière qui permettra d'éviter le pire.
Article original de Silicon

Réagissez à cet article

Original de l’article mis en page : Télégrammes :Darktrace; Google; e-Privacy; backdoor Mac

---

Ce qui changera après l’adoption du règlement général sur la protection des données

Ce qui changera après l’adoption du règlement général sur la protection des données

---

La Cnil a mis en ligne, le 15 juin dernier, une de ses synthèse qui facilitent, même pour les juristes, lappréhension intellectuelle dune nouvelle législation, en loccurrence le désormais célèbre « Règlement général sur la protection des données », puisque tel est le nom raccourci officiel du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à légard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (notre actualité du 4 mai 2016).

À très grands traits, selon la Cnil :

« La réforme de la protection des données poursuit trois objectifs :
• Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
• Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;
• Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées. »
Source : « Règlement européen sur la protection des données : ce qui change pour les professionnels », Cnil, 15 juin 2016.
S'ensuit une série de chapitres présentant les diverses facettes des quelque 173 considérants et 99 articles du règlement ainsi décrypté :
• Un cadre juridique unifié pour l'ensemble de l'UE
• Un renforcement des droits des personnes
• Une conformité basée sur la transparence et la responsabilisation
• Des responsabilités partagées et précisées
• Le cadre des transferts hors de l'Union mis à jour
• Des sanctions encadrées, graduées et renforcées
• Comment les autorités de protection se préparent-elles ?

Peu de changements en vérité…

Signalons, pour ceux qui s'imagineraient que tout change puisque le nouveau règlement abroge toutes les lois de protection des données des États membres de l'Union, que les changements sont en fait fort peu nombreux et que le cadre de protection, surtout tel que nous le connaissions depuis la réforme de notre loi du 6 janvier 1978 sous l'influence de l'ancienne directive 95/46 CE, en date du 1er août 2004. Ce sont les mêmes fondements qui ont présidé à l'élaboration de ces règles communes, automatiquement insérés dans le droit national des États membres.

…Mais des changements piégeant à la marge

Mais cependant, il faut s'attendre à des changements, d'autant plus subreptices qu'ils interviennent dans un océan de stabilité.
On pourrait distinguer deux ordres de dispositions modificatrices :
• Les dispositions qui sont réellement nouvelles, comme par exemple, en France, la disparition des déclarations préalables à la Cnil et quelques autres dispositions vraiment nouvelles ;
• Les dispositions qui existaient déjà dans l'ancienne directive mais qui n'avaient pas été transposées dans la loi d'un pays membre. C'est par exemple le cas du droit à l'oubli dans la loi allemande.

Une marge de manœuvre résiduelle

Cependant, il reste dans le règlement, une certaine latitude d'action de la part des États membres. On peut le comprendre techniquement en comparant un règlement européen à une loi nationale, ce qu'il est effectivement. Il faut donc prendre en compte le fait que chaque pays pourra selon sa sensibilité prendre les mesures d'application de ce règlement – sous forme de décrets en France – ce qui aura de nouveau pour effet d'introduire des divergences de régime d'un pays à l'autre.

Article original de Didier Frochot

Réagissez à cet article

Original de l'article mis en page : Le règlement général sur la protection des données : ce qui change en Europe

---

Quelques chiffres sur les risques du WiFi public

Quelques chiffres sur les risques du WiFi public

Aéroports, hôtels, cafés… Le WiFi public est très utilisé, mais pas sans risque. 30 % des managers ont fait les frais d'un acte cybercriminel lors d'un voyage à l'étranger, selon Kaspersky Lab.

Spécialiste des solutions de sécurité informatique, Kaspersky Lab publie les résultats d'une enquête réalisée par l'agence Toluna auprès de 11 850 salariés, cadres et dirigeants dans 23 pays, sur leur utilisation de terminaux et Internet à l'étranger. Tous ont voyagé à l'international l'an dernier, à titre professionnel ou personnel. Premier constat : 82 % ont utilisé des services WiFi gratuits, mais non sécurisés (aucune authentification n'étant nécessaire pour établir une connexion réseau), depuis un aéroport, un hôtel, un café… Or, 18 % des répondants, et 30 % des managers, ont fait les frais d'un acte cybercriminel (malware, vol de données, usurpation d'identité…) lorsqu'ils étaient à l'étranger.

Droit ou devoir de déconnexion ?

« Les businessmen assument que leurs terminaux professionnels sont plus sûrs du fait de la sécurité intégrée », a souligné l'équipe de Kaspersky Lab dans un billet de blog. Et si cela n'est pas le cas, ils considèrent que ce n'est pas leur problème. Ainsi *« un répondant sur quatre (et plus de la moitié des managers) pense qu'il est de la responsabilité de l'organisation, plutôt que de celle de la personne, de protéger les données. En effet, à leurs yeux, si les employeurs envoient du personnel à l'étranger, ils doivent accepter tous les risques de sécurité qui vont avec »*.

Si des données sont perdues ou volées durant leur voyage, la plupart des managers seraient prêts à blâmer leur département informatique. Et ce pour ne pas avoir recommandé l'utilisation de moyens de protection comme un réseau privé virtuel (VPN), des connexions SSL ou encore la désactivation du partage de fichiers lors d'une connexion WiFi… Quant au droit à la déconnexion, lorsqu'il existe, il se pratique peu. Pour 59 % des dirigeants et 45 % des managers *« intermédiaires »*, il y une attente de connexion quasi continue de la part de leur employeur.

Article original de Ariane Beky,

Réagissez à cet article

Original de l'article mis en page : Les voyageurs d'affaires ignorent les risques du WiFi public

Peut-on communiquer les données personnelles du défunt à ses ayants droit ?

Peut-on communiquer les données personnelles du défunt à ses ayants droit ?

Toute personne physique justifiant de son identité a le droit dobtenir la communication des données personnelles qui la concernent. En revanche, est exclue la communication de ces données aux ayants droit qui ne sauraient être regardés comme des « personnes concernées ».

Mme et MM. D., ayants droit de Mme E. D., décédée le 2 août 2012, ont demandé à la Banque de France, dernier employeur de la défunte, la communication du relevé des derniers appels téléphonique qu'elle avait passé avec le corps médical avant son décès.
Après le refus de la Banque de France, ils ont déposé une plainte le 1er février 2013 auprès de la Cnil.
La Cnil ayant confirmé le refus de la Banque de France dans une décision du 29 mai 2013, ils saisissent le tribunal administratif de Paris qui, par un jugement du 9 décembre 2014, a directement transmis cette requête au Conseil d'Etat.

Le Conseil d'Etat se prononce dans un arrêt du 8 juin 2016.
Il rappelle qu'aux termes du dernier alinéa de l'article 2 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, « la personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement ».
En outre, aux termes de l'article 39 de cette même loi, « toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir (…) la communication, sous une forme accessible, des données à caractère personnel qui la concernent (…) ».
Ainsi, il résulte de ces dispositions qu'elles ne prévoient la communication des données à caractère personnel qu'à la personne concernée par ces données. C'est donc à bon droit que la présidente de la Cnil a pris la décision attaquée à l'égard de Mme et MM. D., qui ne pouvaient, en leur seule qualité d'ayants droit, être regardés comme des « personnes concernées ».
Article original de Céline Solomides

Réagissez à cet article

Original de l'article mis en page : Impossibilité de communiquer les données personnelles du défunt à ses ayants droit

Les géants d’internet contrôlent de plus en plus l’information

Les géants d’internet contrôlent de plus en plus l’information

Entre les médias et les lecteurs, l'information passe aujourd'hui le plus souvent par les algorithmes des géants d'internet, qui contrôlent de fait ce flux et une bonne partie des revenus qu'il génère. Au point de susciter des inquiétudes.

« Ces 18 derniers mois, (ces géants d'internet) qui avaient jusqu'ici une relation distante avec le journalisme sont devenus des acteurs dominants de l'écosystème de l'information », résume le Tow Center for Digital Journalism de l'Université américaine de Columbia, dans une étude publiée en juin 2016. Beaucoup proposent aux éditeurs de presse de publier directement leur contenu sur leurs plateformes, à l'instar des canaux Instant Articles de Facebook ou Discover de Snapchat, et sont*« désormais directement impliqués dans tous les aspects du journalisme »*, fait valoir l'étude. La plupart des médias nouent des partenariats avec ces nouveaux acteurs de l'information pour maintenir ou développer leur exposition sur les moteurs de recherche et les réseaux sociaux, mais les perspectives financières restent incertaines.
« Il y a des gens qui font de l'argent sur internet, mais pas les médias, qu'ils soient tous supports ou uniquement en ligne », affirme une autre étude, du centre indépendant Pew Research Center, publiée mi-juin. Elle souligne ainsi qu'en 2015, 65% des revenus publicitaires en ligne étaient concentrés par cinq places fortes du web, Google, Facebook, Microsoft, Yahoo et Twitter, une proportion en hausse par rapport à 2014 (61%). Tout comme le modèle économique, c'est aussi le contenu et sa hiérarchie qui leur échappent, soumis au filtre des algorithmes. *« L'impact que ces sociétés technologiques ont sur le secteur du journalisme va bien au-delà de l'aspect financier, jusqu'à ses composantes les plus essentielles »*, considère l'institut Pew.
Désormais, les géants d'internet *« supplantent les choix et les objectifs des sites d'information et leurs substituent (les leurs) »*, affirme l'étude. Si certains y voient l'occasion d'une démocratisation de l'information, d'autres s'inquiètent d'une altération de sa qualité. *« Vous n'avez aucune idée de ce que les gens vont voir et il se peut tout à fait que (ce soit) quelque chose d'assez léger plutôt que des informations majeures »*, prévient Dan Kennedy, professeur de journalisme à l'Université Northeastern.

Le secret des algorithmes

Une étude réalisée par Nic Newman du Reuters Institute a fait état de*« préoccupations liées à la personnalisation des informations et une sélection algorithmique qui pourraient passer à côté de nouvelles importantes et de points de vue différents »*, selon le blog de son auteur. Mais *« les jeunes préfèrent les algorithmes aux éditeurs »* qui organisent l'information, constate-t-il. Ce pouvoir croissant des incontournables d'internet a attiré l'attention début mai lorsque le site d'information Gizmodo a accusé, témoignages à l'appui, Facebook d'avoir manipulé son fil de tendances. Après enquête interne, le plus grand réseau social du monde a conclu qu'il n'y avait pas eu de démarche concertée ou de manipulation, mais s'est engagé à préserver la neutralité de sa plateforme.
« Nous sommes une entreprise technologique, pas un média », a expliqué récemment la directrice d'exploitation de Facebook, Sheryl Sandberg, lors d'une table ronde à Washington. *« Nous n'essayons pas de recruter des journalistes ou de rédiger des nouvelles »*, a-t-elle martelé. Pour autant, l'intervention humaine reste nécessaire, selon elle, *« parce que sans cela, tous les jours à midi, le déjeuner serait une tendance »*. Même si la hiérarchisation des informations est largement automatisée sur ces plateformes, les programmes qui régissent ce processus sont bien rédigés par des humains qui opèrent, pour ce faire, des choix. Cela pose, dès lors,*« des questions quant à la transparence »* de l'ensemble, souligne Nicholas Diakopoulos, professeur de journalisme à l'université du Maryland. *« Il pourrait être intéressant de savoir de quelles données se nourrit le logiciel ou quels sites il suit »*, estime l'universitaire, pour qui *« il faut réfléchir à des normes de transparence ».*
Une étude publiée l'an dernier a révélé que le trafic des principaux sites d'information en provenance de Facebook avait chuté de 32% après une modification des algorithmes du réseau social. *« Il est vrai que Facebook peut faire décoller ou tuer un site d'information selon la façon dont il calibre son algorithme »*, reconnaît Nikki Usher, professeure de nouveaux médias à l'Université George Washington. *« D'un autre côté, les médias n'ont jamais eu à rendre de compte sur les décisions qu'ils prenaient »* en matière éditoriale, fait-elle valoir.

Article original de Joël Ignasse

Réagissez à cet article

Original de l'article mis en page : Les géants d'internet contrôlent de plus en plus l'information – Sciencesetavenir.fr

Les magistrats du palais de justice de Ouagadougou outillés pour combattre la cybercriminalité

	Les magistrats du palais de justice de Ouagadougou outillés pour combattre la cybercriminalité

La Commission de l'Informatique et des Libertés (CIL) en partenariat avec les tribunaux du palais de justice de Ouagadougou, organise un séminaire de sensibilisation des magistrats et greffiers du palais de justice de Ouagadougou aux « enjeux de la protection des données personnelles et de la vie privée des citoyens à l'ère du numérique ». Ce séminaire se déroule à Ouagadougou ce mardi 28 juin 2016.

« Aucune personne n'est, de nos jours, à l'abri des actes cybercriminels, quel que soit son statut, son rang ou l'état de ses connaissances », a lancé Marguerite Ouédraogo/Bonané, présidente de la CIL. Si de nos jours la cybercriminalité avance à grand pas dans le monde entier, force est de constater que les initiatives pour l'affronter ne manquent pas. La lutte contre cette nouvelle forme de criminalité impose donc que de « nouvelles approches soient développées et que toutes ses dimensions soient maitrisées », a-t-elle reconnu. Dans l'optique de protéger les données des justiciables en justice, la CIL entend informer et sensibiliser les magistrats aux droits des personnes dont les données sont utilisées. « Notre mission aujourd'hui c'est de les informer et de les sensibiliser aux droits des personnes dont les données sont utilisées », a confié marguerite Ouédraogo/Bonané. A l'en croire, la protection des données couvre tout le territoire. Par conséquent, tous les Burkinabé sont concernés par cette protection. Elle révèle que ce séminaire ouvert aux magistrats permettra à ces derniers de protéger les données des justiciables comme le stipule « notre loi ».

Des communications qui seront faites dans ce séminaire

Plusieurs communications seront faites durant ce séminaire. En substance, une communication sera faite à l'intention des magistrats pour leur faire connaitre le cadre juridique et institutionnel des données personnelles au Burkina Faso. Une autre sera de leur faire connaitre la communication sur l'enquête judiciaire et la protection des données personnelles face à l'enquête judiciaire. Aussi, la formation sur l'utilisation de l'internet et des réseaux sociaux leur sera-t-elle donnée.

Vu l'importance de ce séminaire qui est focalisé sur les acteurs de la justice, Dieudonné Manly, Conseiller Technique du ministère de la justice, accorde un peu plus de crédit à l'ordre du jour quand il affirme qu' « aujourd'hui la cybercriminalité a pris de l'ampleur et il va falloir outiller les magistrats afin qu'ils puissent faire face à ce phénomène ». Aussi, pense-t-il que les thèmes choisis sont bien réfléchis et que ces thèmes vont, à son avis, « permettre aux magistrats de faire face à la cybercriminalité ».

Article original de Armand Kinda

Réagissez à cet article

Original de l’article mis en page : Lutte contre la cybercriminalité : les magistrats du palais de justice de Ouagadougou outillés pour en faire face