Le droit à l’oubli comment ça marche ?

	Le droit à l’oubli comment ça marche ?

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

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

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

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

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

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

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

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

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

---

Faille d'iCloud : Apple avait-il été alerté depuis

des mois ?

	**Faille d’iCloud : Apple avait-il été alerté depuis des mois ?**

Au début du mois, Apple a été sévèrement mis en cause suite au vol et à la publication sur Internet de photos intimes de nombreuses célébrités américaines. La firme a assuré que ses serveurs n'avaient pas été piratés et promis une meilleure protection à l'avenir.

Or selon The Daily Dot, cet incident aurait pu être évité. Comment ? En corrigeant bien plus tôt une faille de sécurité d'iCloud. Car cette vulnérabilité serait celle finalement corrigée fin août. Pourtant, celle-ci aurait été signalée à deux reprises à Apple par un chercheur en sécurité, Ibrahim Balic.

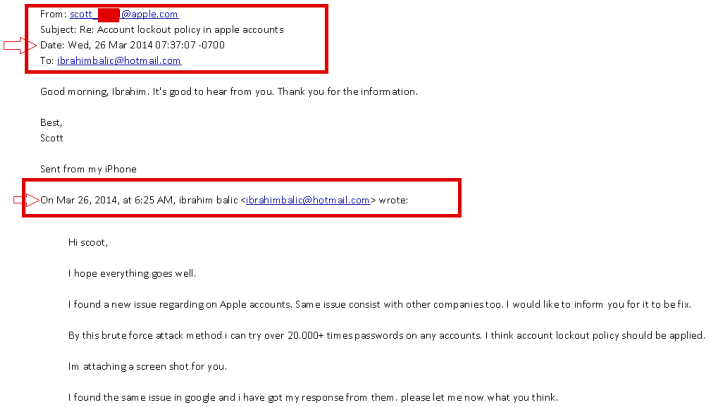
Apple réfute tout lien entre la faille et le vol des photos

Comme l'attestent des emails publiés par le Daily (ci-dessous), l'expert a informé Apple dès le 26 mars d'une méthode permettant d'exécuter une attaque en « brute force » afin de forcer l'accès à un compte iCloud.

Il était en effet possible de tester de très nombreuses combinaisons pour se connecter, Apple n'ayant pas introduit de limitations du nombre de tentatives autorisées. Balic expliquait ainsi avoir pu essayer plus de 20.000 mots de passe.

Début mai, la vulnérabilité ne semblait toujours pas corrigée, l'équipe sécurité d'Apple continuant d'interroger le chercheur sur sa découverte et jugeant par ailleurs la méthode de Balic trop longue pour accéder effectivement de manière illicite à un compte.

Cette faille au niveau de la fonction « Localiser mon iPhone » a-t-elle permis de dérober des photos sur iCloud ? Apple a réfuté tout lien et affirmé que ces divulgations résultaient uniquement d'attaques ciblées contre les victimes.



From : scott_[redacted]@apple.com
Subject: Re: Account lockout policy in apple accounts
Date: Wed, 26 Mar 2014 07:37:07 -0700
To: ibrahimbalic@hotmail.com

Good morning, Ibrahim. It's good to hear from you. Thank you for the information.

Best,
Scott

Sent from my iPhone

On Mar 26, 2014, at 6:25 AM, ibrahim balic <ibrahimbalic@hotmail.com> wrote:

Hi scoot,

I hope everything goes well.

I found a new issue regarding on Apple accounts. Same issue consist with other companies too. I would like to inform you for it to be fix.

By this brute force attack method i can try over 20.000+ times passwords on any accounts. I think account lockout policy should be applied.

Im attaching a screen shot for you.

I found the same issue in google and i have got my response from them. please let me now what you think.

Ibrahim Balic 26-Mar-2014 09:21 PM

Hi Again,

Same issue here:

GET https://p05-mailws.icloud.com:443/wm/ext/sendfrom HTTP/1.1
Host: p05-mailws.icloud.com:443
Connection: keep-alive
Proxy-Connection: keep-alive
Accept: */*
If-Modified-Since: Mon, 24 Mar 2014 00:18:15 Eastern European Standard Time
User-Agent: iPhone Mail (11D167)
Authorization: X-MobileMe-AuthToken base64(userid:password) // MTA[redacted]
Accept-Language: en-us
Accept-Encoding: gzip, deflate

Ibrahim Balic 26-Mar-2014 03:34 PM

Summary:
hi guys,

I found a method for brute-force attack. I found the same issue in google and I've tried 20.474 times password to any account. Account is not locked, malicious people can be exploit here.

"Authorization" parameter in header allowed userid and user password. (with base64 encode)

POST https://p05-keyvalueservice.icloud.com/sync HTTP/1.1
Host: p05-keyvalueservice.icloud.com
Accept: */*
X-Apple-Request-UUID: [redacted]
Authorization: X-MobileMe-AuthToken base64(userid:userpassword)
Content-Encoding: gzip
Proxy-Connection: keep-alive
X-MMe-Client-Info: <iPhone6,1> <iPhone OS;7.1;11D167> <com.apple.SyncedDefaults/166.7>
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-us
X-Apple-Scheduler-ID: com.apple.syncedpreferences
Accept-Encoding: gzip, deflate
User-Agent: SyncedDefaults/166.7 (iPhone OS;7.1 (11D167))
Content-Length: 395
Connection: keep-alive

Steps to Reproduce:

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

Source :
http://www.zdnet.fr/actualites/faille-d-icloud-apple-avait-il-ete-alerte-depuis-des-mois-39806921.htm
Apple warned of iCloud brute-force vulnerability 6 months before Celebgate

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

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

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

Si Google a l'obligation, suite à une décision de justice européenne, d'appliquer le droit à l'oubli pour les internautes qui en font la demande, ses méthodes ne font pas l'unanimité. Le moteur a d'ailleurs été récemment condamné par le Tribunal de Grande Instance de Paris à retirer les contenus diffamatoires de ses résultats de recherche.
Google fera probablement appel de cette décision, la question de la portée des déréférencements étant un sujet de débat entre l'entreprise et les différentes Cnil européennes.
La Cnil française justement juge assez sévèrement l'attitude de Google en la matière. Dans un entretien au Figaro, Isabelle Falque-Pierrotin, présidente de la Commission nationale informatique et libertés explique : « Les demandes d'effacement sont prévues par la loi depuis longtemps et sont appliquées par les possesseurs de sites. Google n'était pas considéré comme responsable du traitement de données personnelles ».

Replacer la Cnil au coeur du dispositif
Et d'asséner : « Il y a beaucoup d'habileté et de malice de la part de Google pour entretenir la confusion et discréditer ce droit à l'oubli. Il faut se positionner dans ce débat sans ouvrir le front des menaces de censure. Le droit au déréférencement est complexe. Il faut trouver un équilibre, avec finesse ».
Rappelons que jeudi 25 septembre 2014, s'est tenu à Paris une réunion organisée par Google sur cette question. La Cnil y a assisté en tant qu' »observateur ».
La Commission rappelle d'ailleurs qu »en cas de refus de Google, les Français peuvent saisir la Cnil d'une plainte, en décrivant leur demande et la réponse qu'il ont obtenue. Nous avons reçu une soixantaine de plaintes, que nous allons examiner, avant d'ordonner ou non à Google de retirer ces liens. Nous avons toutefois demandé à ces personnes de patienter, car nous souhaitons nous coordonner avec les autres autorités européennes, pour définir des règles communes ».
Replacer la Cnil au centre de l'exercice du droit à l'oubli est aussi une volonté du gouvernement. Interrogée par ZDNet.fr, Axelle Lemaire, secrétaire d'Etat au Numérique souligne : « Le rôle de la CNIL doit être redéfini, le modèle proposé par Google ne me convient pas ».

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

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

---

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

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

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

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

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

Le bal des jurisprudences peut commencer

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

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

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

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

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

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

Après le BYOD, voici le WYOD

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

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

Un phénomène qui pourrait bien se généraliser

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

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

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

Bientôt invisibles à nos yeux

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

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

Que faire ? Les interdire ?

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

Le contrôle avant tout

Plutôt qu'interdire, mieux vaut donc disposer d'une véritable politique propre à tous les appareils, y compris donc les objets et vêtements intelligents et connectés. Mieux vaut ainsi avoir le contrôle et la mainmise sur ce type de produits qu'en ignorer la présence, ce qui est la pire des situations.

Qui plus est, comme pour les smartphones, les entreprises doivent en tirer profit, que ce soit pour communiquer avec leurs employés ou encore trouver un moyen d'exploiter ces objets vis-à-vis des clients. Après tout, il s'agit de produits souvent compatibles avec d'autres appareils, et il n'est pas rare qu'un important espace de stockage en ligne (cloud) l'accompagne. Si cela peut devenir un problème, cela peut donc surtout être un atout.

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

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

Source :

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

Par Nil Sanyas

Dix-huit anglicismes dans le domaine informatique ont désormais leur équivalent français

Dix-huit anglicismes dans le domaine informatique ont désormais leur équivalent français

La Commission générale de terminologie a encore sévi. Par décret, elle préconise d'utiliser une série d'équivalents français à dix-huit anglicismes dans le domaine informatique. Le back office devient un arrière-guichet et – logique – le front office un guichet. Les framework et integrated development environment (IDE) se transforment respectivement en environnement de développement et en atelier de développement.

Un thumbnail (image réduite par rapport à l'original) prend le joli nom d'imagette et le lurker (internaute qui suit les échanges sur le web sans y participer) celui de fureteur. Proches des termes originaux, le blogue, le microblogue ou la cyberconférence ont plus de chances de remplacer, dans l'usage courant, le blog, le microblogging ou la web conference.

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

Source :
http://www.01net.com/editorial/626898/ne-dites-plus-back-office-mais-arriere-guichet/#?xtor=EPR-1-NL-01net-Actus-20140916

Le système de reconnaissance biométrique du FBI est

opérationnel

Le système de reconnaissance biométrique du FBI est opérationnel

Grâce aux outils du système NGI, le FBI pourra retrouver des criminels dans tous les Etats-Unis grâce à une empreinte, un scan d'iris ou une photo.

Le système NGI sera disponible dans tous les Etats-Unis d'ici à la fin 2014.
Après trois années de développement, le nouveau système de reconnaissance biométrique Next Generation Identification system) du FBI est opérationnel a annoncé le Bureau le 15 septembre 2014. Il a été conçu pour améliorer les possibilités d'identification biométriques explique le FBI dans son communiqué.
Il comporte deux nouveaux outils qui viennent s'ajouter aux bases de données d'empreintes digitales et de scans d'iris. Le premier concerne la reconnaissance faciale, l'Interstate Photo System (IPS) et le second, Rap Back, fournit des notifications écrites.

La base contiendra à terme 52 millions de photos.

Rap Back permet à toutes les autorités habilitées de recevoir des informations sur l'historique criminel de toute personne occupant un poste de confiance : un professeur, un conseiller bancaire…, explique le FBI dans son communiqué. Plus question de passer sous silence une arrestation pour conduite en état d'ivresse à 19 ans. Quant à IPS, il permet d'accélérer la recherche de criminels grâce à une base de données qui comptera 52 millions de photos d'ici à 2015.

En avril dernier, l'ONG Electronic Frontier Foundation émettait déjà quelques réserves sur cet outil. En premier lieu, elle dénonçait le mélange des genres puisqu'en plus des photos de criminels, celles de citoyens lambdas se trouvaient dans cette base. Elle s'inquiétait également du risque de « faux positif » compte tenu du taux de fiabilité du système qui n'est que de 85 %.

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

Source :
http://www.01net.com/editorial/626932/le-systeme-de-reconnaissance-biometrique-du-fbi-est-operationnel/#?xtor=EPR-1-NL-01net-Actus-20140916

Cécile Bolesse

Droit à l'oubli : Une vue générale des demandes de désindexation à Google

Droit à l'oubli : Une vue générale des demandes de désindexation à Google

Google reste assez évasif sur les demandes qui lui sont adressées chaque jour au titre du droit à l'oubli, instauré par la décision prise par la CJUE en mai. On sait certes que le nombre de demandes traitées par le géant des moteurs de recherche est important, au moins 120.000 requêtes ont été adressées à Google depuis l'ouverture de son formulaire. Mais derrière les chiffres officiels se cache une vraie bataille politique menée par Google autour de ce droit à l'oubli et la firme de Mountain View distille ses informations sur le sujet avec précaution.

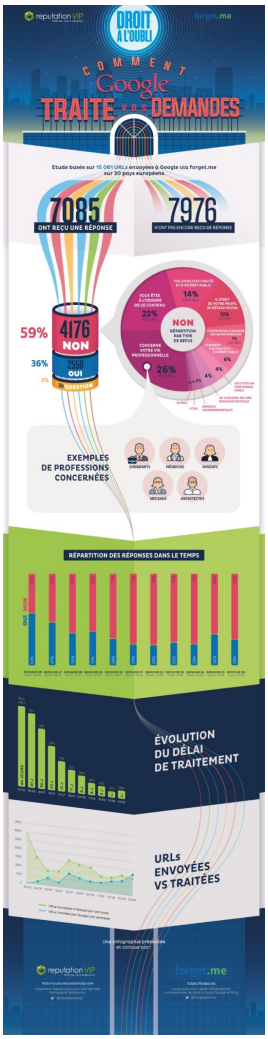
Forget.me est un site qui se propose comme un intermédiaire entre l'utilisateur lambda et le formulaire de Google.
Au total, depuis le lancement de son service, Forget.me a reçu plus de 15.000 demandes (depuis 30 pays d'Europe) dont environ la moitié a été traitée par Google. L'entreprise a donc compilé ses résultats et publie une étude retraçant leur vision de ce phénomène.

Lors de la mise en place de son service, en juin, Forget.me a ainsi reçu environ 1800 demandes de déréférencement. A l'époque, Google répondait en moyenne à une demande en 44 jours mais aujourd'hui, soit environ 3 mois plus tard, le nombre de demande par semaine semble stabilisé aux alentours de 300 et Google répond en moyenne en moins de 4 jours.

Autre statistique relevée par Forget.me : Google semble bien plus difficile sur les demandes que lors du lancement du service. En juin, le taux de refus de la part du moteur de recherche était autour de 50%, aujourd'hui celui-ci flirte plus souvent avec les 70%. Le moteur de recherche s'appuie pour cela sur 11 typologies de refus. La plus fréquente étant « Concerne votre vie professionnelle » avec 26% des URL concernées.

« Plusieurs facteurs entrent en jeu, et Google n'est pas le seul en cause dans ce durcissement » précise Bertrand Girin « Il est possible que Google ait volontairement durci ses critères, mais ce droit est encore jeune et ses équipes ont probablement eu besoin de s'adapter et de se former pour le maitriser totalement. Et cela prend évidemment un peu de temps. » Même constat pour les différentes Cnils européennes, qui doivent bientôt publier leurs directives sur le sujet, le droit va s'adapter à cette nouvelle régulation et les usages vont se stabiliser.

Pour visualiser ces indicateurs, Reputation VIP a eu la bonne idée de créer une infographie synthétique :



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

Source :
http://www.zdnet.fr/actualites/droit-a-l-oubli-vers-une-stabilisation-des-demandes-a-google-en-europe-39806691.htm

Rapport 2013 DU GIABA : trafic de drogue, fraude fiscale, cybercriminalité constituent les infractions les plus fréquentes au Sénégal

Rapport 2013 DU GIABA : trafic de drogue, fraude fiscale, cybercriminalité constituent les infractions les plus fréquentes au Sénégal

Le Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest (Giaba) vient de publier son rapport annuel pour l'année 2013, dans lequel, il souligne que le trafic de drogue, la fraude fiscale, les autres investissements et la cybercriminalité ont été les infractions sous-jacentes les plus fréquentes en 2013.

Le rapport annuel 2013 du Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest (Giaba) vient d'être publié. En ce qui concerne notre pays, le Giaba a signalé que «le rapport national du Sénégal répertorie le trafic de drogue, la fraude fiscale, les autres investissements et la cybercriminalité comme infraction sous-jacentes les plus fréquentes en 2013». Il a aussi rappelé que «le rapport de l'Organe international de contrôle des stupéfiants (Incsr) 2013 du développement d'Etat américain étend la liste pour y inclure les fraudes bancaires et de dépôt, la falsification de documents, la revente de voitures volées et les combines de la Ponzi. Un taux de corruption élevé a également été signalé dans le pays, un phénomène qui frappe tous les niveaux de gouvernance et le commerce, selon le rapport ».
Le Giaba a souligné que «le Sénégal a de plus en plus démontré son engagement à lutter contre les crimes financiers, y compris le Bc/Ft» surtout en prenant des mesures pour renforcer son dispositif de lutte contre le blanchiment des capitaux et de lutte contre le financement du terrorisme (Lbc/Ft). Cependant, «Un projet de stratégie national de Lbc/Ft est actuellement en attente d'approbation par les autorités, conformément à la loi de Lbc/Ft».
Le rapport annuel renseigne aussi que, chez nous, «plusieurs décisions de justice ont été rendues, y compris des peines d'emprisonnement, des amendes et confiscations, suite à des accusations de blanchiment de capitaux». Et en 2013, la Cellule de renseignement financier a reçu 109 déclarations d'opérations suspectes liées au blanchiment, 14 des cas analysés ont été envoyés aux autorités d'exécution, aux fins d'enquête et de poursuite et 3 condamnations ont été prononcées. Il faut dire que dans les premières lignes de la partie du rapport consacré à notre pays, la traduction en justice, pour enrichissement illicite de Karim Wade, a été rappelée : «En 2013, la répression de la corruption a conduit à la mise en accusation devant les tribunaux de plusieurs ministres dans le gouvernement du Président Wade, dont son fils, Karim Wade, pour corruption» y lit-on.
Même si le Sénégal a fait des progrès d'envergure dans le renforcement de son système de Lbc/Ft, les lacunes suivantes demeurent, selon le Giaba «l'adoption d'un cadre approprié de l'approche fondée sur les risques, la mise en oeuvre de mesures de vigilance pour la surveillance continue des relations et transaction avec les clients, la conduite de l'application de mesures renforcées de vigilance pour les clients à risques élevés».
Egalement, «le renforcement de l'obligation de déclarer les tentatives d'opération et un mécanismes pour la mise en oeuvre des résolutions 1267 et 1373 du conseil de sécurité de l'Onu et les résolutions qui les ont suivies».

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

Source :
http://www.dakaractu.com/Rapport-2013-DU-GIABA-trafic-de-drogue-fraude-fiscale-cybercriminalite-constituent-les-infractions-les-plus-frequentes_a73269.html

Données personnelles : la Cnil épingle l’opacité des applis mobiles

Données personnelles : la Cnil épingle l’opacité des applis mobiles

Près de 15% de 121 applications examinées ne fournissent aucune information sur le traitement des données collectées et la moitié rendent ces infos peu accessibles.

La collecte de données personnelles par les applis mobiles téléchargées ne donne pas lieu à beaucoup d’informations de la part de leurs éditeurs. C’est le constat issu d’une démarche initiée, en mai 2014, par la Cnil et 26 de ses homologues dans le monde. Celles-ci ont mené un audit en ligne simultané de plus de 1 200 applications mobiles gratuites et payantes.
Leurs vérifications ont porté sur le type de données collectées par les applications, le niveau d’information des utilisateurs et la qualité des explications données par l’application concernant le motif de la collecte de ces données.
Pour la France, la Cnil a examiné 121 applications parmi les plus populaires pour les trois principaux systèmes d’exploitation mobiles (iOS, Android, Windows Phone). Ses conclusions ne diffèrent pas du constat général effectué à l’échelon mondial.
La CNIL a passé au crible 121 applications mobiles les plus populaires en France
Ainsi, 15% des applications examinées ne fournissent aucune information sur le traitement des données collectées. Et même lorsqu’une information est fournie sur la politique de collecte, près de la moitié des applications concernées ne la rendent pas facilement accessible.
La Cnil déplore qu’on impose à l’utilisateur une recherche active sur le site internet de l’éditeur ou dans les différents onglets de l’application : « Il a ainsi été constaté que les mentions d’information de certaines applications à destination d’utilisateurs français ne sont disponibles qu’en anglais. »
Fort des de constat, la Commission recommande aux utilisateurs d’être à la fois curieux, vigilants et exigeants. « Il existe un large choix d’applications offrant des services similaires, détournez vous de celles qui en demandent le plus et en disent le moins ! » conclut-elle.

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

Source :
http://www.01net.com/editorial/626952/donnees-personnelles-la-cnil-epingle-lopacite-des-applis-mobiles/#?xtor=EPR-1-NL-01net-Actus-20140917
Frédéric Bergé 01net.le 16/09/14 à 19h50