

Skype sur écoute : un amendement de la loi Macron relance le débat | Le Net Expert Informatique



Le débat sur la qualification de Skype et de certains autres services de VoIP en tant qu'opérateurs de téléphonie devrait repartir. Un amendement contenu dans la loi Macron souhaiterait que ce type d'outil dispose des mêmes obligations que les opérateurs classiques.

Un amendement contenu dans le projet de loi Macron pourrait bien relancer le débat autour de la classification de Skype en tant qu'opérateur de téléphonie. Il ne s'agit pas ici d'un simple conflit pour tenter de mettre le service de VoIP dans une case, mais d'obliger le logiciel, propriété de Microsoft, à respecter certaines obligations qui découlent de ce statut.

Parmi ces obligations figurent par exemple le fait de devoir **autoriser les appels d'urgence**, de **financer le service universel** ou encore de **permettre les écoutes téléphoniques**. Dans ce dernier cas, cela supposerait que les services de renseignement français pourraient accéder au logiciel dans le cadre d'enquêtes.

Selon Les Echos, un amendement parlementaire, soutenu par le gouvernement et d'ores et déjà adopté le 7 février à l'Assemblée nationale, confère le droit à l'Arcep de déclarer un tel programme comme un opérateur de télécommunications. Le texte n'est pas encore définitivement adopté puisqu'il doit d'abord être voté par le Sénat.

Si le Parlement vote en sa faveur, l'Arcep pourrait à terme obliger certains programmes de VoIP à respecter leurs obligations sans que le régulateur ne soit obligé de les attaquer en justice au préalable.

Le sujet traîne depuis 2007

Si l'amendement semble récent, le sujet traîne auprès des autorités concernées depuis quelques années. Depuis 2007, l'Arcep souhaite en effet que Skype soit déclaré en tant qu'opérateur de téléphonie en France. Pour l'autorité, le fait que la plateforme propose d'appeler des numéros de téléphonie, fixes ou mobiles via un ordinateur ou un smartphone est une condition permettant de la faire entrer dans cette catégorie.

Une enquête préliminaire aurait même été diligentée sur la question, les investigations étant a priori dirigées par la brigade de répression de la délinquance aux personnes. L'enjeu était alors identique à savoir l'obligation de se plier à des impératifs comme le fait d'autoriser les appels d'urgence, financer le service universel ou encore permettre les écoutes téléphoniques.

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 protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source

<http://pro.clubic.com/legislation-loi-internet/actualite-758733-skype-macron-ecoute.html>

Dématérialisation et aspects juridiques à ne pas négliger | Le Net Expert Informatique



Dématérialisation et aspects juridiques à ne pas négliger

Les points auxquels il faut particulièrement prêter attention dans les CGV : la sécurité et la confidentialité des données, la localisation de ces dernières et les garanties en termes de conservation. Le point avec l'avocate-ingénieur Isabelle Renard.

La dématérialisation est aujourd'hui incontournable dans les entreprises : l'automatisation du procure to pay est en marche. A condition de ne pas négliger les aspects juridiques.

Première chose à laquelle il est nécessaire de faire attention : les conditions générales de vente (CGV) des prestataires d'hébergement en cloud computing. « Pour les contrats de cloud, la logique n'est pas de négocier les contrats. Au contraire, il s'agit de regarder les offres des différents prestataires et de s'assurer qu'elles correspondent bien à ce que l'on recherche », explique Me Isabelle Renard, avocate-ingénieur.

Un travail qu'il n'est pas toujours évident à mener, les CGV de certains prestataires étant volontairement opaques. « Ce sont parfois de vraies poupées russes, un empilement de conditions avec des liens hypertextes... C'est difficile, même pour un juriste », constate Me Renard.

S'attacher aux garanties

Les points auxquels il faut particulièrement prêter attention : la sécurité et la confidentialité des données, la localisation de ces dernières et les garanties en termes de conservation. « Les contrats bas de gamme ne garantissent pas où sont les données et il peut être dangereux de voir certaines données confidentielles sur des serveurs localisés un peu partout dans le monde », insiste Isabelle Renard.

De même, pour les documents qui doivent être conservés longtemps, il est nécessaire de s'assurer que le prestataire pourra le restituer dans un format lisible – qui n'est pas forcément le format d'origine, étant données les évolutions technologiques. « Il est important de ne pas s'attacher qu'au prix des prestations mais aussi aux garanties apportées », résume Me Renard.

L'avocate conseille également de ne pas signer avec un interlocuteur qui n'est pas installé sur le territoire de préférence français, ou a minima européen : « En cas de problèmes judiciaires, cela peut revenir très cher de devoir traiter avec un prestataire étranger, même au sein de l'Union européenne », souligne-t-elle.

Difficile dans les pays hors UE

Avant de se lancer dans la dématérialisation à tout va et dans toutes les filiales – y compris à l'international -, s'assurer également que les documents électroniques sont bien reconnus dans les pays concernés. « Au niveau de l'Union européenne, le règlement européen e-IDAS, qui sera d'application directe en France mi 2016, permet une reconnaissance globale de l'écrit électronique et de la signature électronique. Mais cela peut-être plus difficile dans les pays hors UE, et doit faire l'objet d'une vérification au cas par cas », rapporte Isabelle Renard.

Certaines normes doivent cependant être respectées pour qu'un document électronique soit reconnu. S'assurer que le prestataire sélectionné s'engage bien à les respecter.

Dans ces cas-là, avec un document électronique natif qui apporte une bonne garantie de valeur probante, il n'y a plus besoin de conserver de documents papier. Le tout dématérialisé est réellement en marche.

Consultez l'article rédigé par Denis JACOPINI sur ce thème :

L'utilisation juridique des documents numériques à l'ère de la dématérialisation à outrance

Expert Informatique 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 protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :

<http://www.decision-achats.fr/Thematique/process-outils-1037/Breves/Dematérialisation-aspects-juridiques-pas-negliger-251831.htm>

Comment rendre l'information infalsifiable ? Avec les blockchains | Le Net Expert Informatique



Comment rendre l'information infalsifiable ? Avec les blockchains

On sait maintenant réaliser des supports inscriptibles, partagés et infalsifiables. Ce qu'il est possible d'en faire est étonnant, formidable... et révolutionnaire.

Imaginez qu'à la place de la Concorde à Paris, à côté de l'obélisque, on installe un très grand cahier que, librement et gratuitement, tout le monde puisse lire, sur lequel chacun puisse écrire, mais qui soit impossible à modifier et indestructible. Cela serait-il utile ? Il semble que oui.

On pourrait y consigner des engagements, comme : « Je promets de donner ma maison à celui qui prouvera la conjecture de Riemann ; signé Jacques Dupont, 11 rue Martin à Paris. » On pourrait y déposer la description de ses découvertes, afin qu'il soit impossible d'en être dépossédé. On pourrait y laisser des reconnaissances de dettes, considérées valides tant que le prêteur n'est pas venu indiquer sur le cahier qu'il a été remboursé.

On pourrait y déposer des messages adressés à des personnes qu'on a perdues de vue, en espérant qu'elles viennent les lire et reprennent contact. On pourrait y consigner des faits que l'on voudrait rendre publics définitivement, pour que l'histoire les connaisse, pour aider une personne dont on souhaite défendre la réputation, pour se venger, etc.

Pour que cela soit commode et pour empêcher les tricheurs de prendre des engagements en votre nom ou écrire en se faisant passer pour vous, il faudrait que l'on puisse signer les messages déposés de telle façon que personne ne puisse se substituer à vous. Il serait utile aussi que l'instant précis où est inscrit un texte soit indiqué à chaque fois (horodatage).

Imaginons que tout cela soit possible et qu'un tel cahier soit mis en place, auquel s'ajouteraient autant de pages nouvelles que nécessaire. Testaments, contrats, certificats de propriétés, messages publics ou adressés à une personne particulière, attestations de priorité pour une découverte, etc., tout cela deviendrait facile sans notaire ni huissier. Un tel cahier public, s'il était permanent, infalsifiable, indestructible et qu'on puisse y écrire librement et gratuitement tout ce qu'on veut, aurait une multitude d'usages.

Public, infalsifiable et indestructible

Un tel objet serait plus qu'un cahier de doléance ou un livre d'or, qui peuvent être détruits. Plus qu'un tableau d'affichage offert à tous sur les murs d'une entreprise, d'une école ou d'une ville, eux aussi temporaires. Plus que des enveloppes déposées chez un huissier, coûteuses et dont la lecture n'est pas autorisée à tous. Plus qu'un registre de brevets, dont la permanence est assurée, mais sur lesquels il est difficile d'écrire. Plus que les pages d'un quotidien, indestructibles car multipliées en milliers d'exemplaires, mais auxquelles peu de gens ont accès et dont le contenu est très contraint.

Bien sûr, ce cahier localisé en un point géographique unique ne serait pas très commode pour ceux qui habitent loin de Paris. Bien sûr, ceux qui y rechercheraient des informations en tournant les pages se gêneraient les uns les autres et gêneraient ceux venus y inscrire de nouveaux messages. Bien sûr encore, faire des recherches pour savoir ce qui est écrit dans le cahier deviendrait impossible en pratique quand le cahier serait devenu trop gros et que ses utilisateurs se seraient multipliés.

Ces trois inconvénients majeurs – localisation unique rendant l'accès malcommode et coûteux, impossibilité d'y lire ou écrire en nombre au même instant, difficultés de manipuler un grand cahier – peuvent être contournés. L'informatique moderne, avec la puissance de ses machines, y compris les smartphones et ses réseaux de communication, est en mesure de les surmonter.

Cette idée d'un grand cahier informatique, partagé, infalsifiable et indestructible du fait même de sa conception est au cœur d'une nouvelle révolution, celle de la blockchain, ou plus explicitement et en français : la révolution de la programmation par un fichier partagé et infalsifiable.

Une idée mise en œuvre pour les bitcoins

Le terme blockchain vient du bitcoin, la monnaie cryptographique créée en janvier 2009 et qui a depuis connu un développement considérable et un succès réel, la valeur d'échange des bitcoins émis dépassant aujourd'hui deux milliards d'euros. Au cœur de cette monnaie, il y a effectivement un fichier informatique infalsifiable et ouvert. C'est celui de toutes les transactions, et son inventeur Satoshi...

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 protection juridique du chef d'entreprise.

Contactez-nous

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

Source : http://www.pourlascience.fr/ewb_pages/a/article-les-blockchains-clefs-d-apos-un-nouveau-monde-33873.php
Par Jean-Paul Delahaye et Philippe Boulanger

Piratage de plans de réacteurs nucléaires : le

hacker fait du chantage | Le Net Expert Informatique

x	Piratage de plans de réacteurs nucléaires : le hacker fait du chantage
---	--

SEOUL, 12 mars (Yonhap) – Le pirate informatique qui a rendu publics des plans de réacteurs nucléaires du pays à la fin de l'année dernière a fait ce jeudi du chantage, demandant de l'argent en contrepartie de sa promesse de ne pas dévoiler d'informations sensibles à des pays tiers.

Utilisant un compte sous le nom de président du soi-disant groupe antinucléaire, le hacker a posté 25 nouveaux fichiers sur Twitter qui incluraient des documents sur le réacteur 1400 développé par la Corée du Sud.

«Besoin d'argent. Vous n'avez qu'à répondre à quelques demandes. [...] De nombreux pays d'Europe du Nord, d'Asie du Sud-Est et d'Amérique du Sud disent qu'ils achèteront des informations sur le réacteur nucléaire. Peur que la vente de la totalité des informations ne détruise les efforts de la présidente Park (Geun-hye) visant à exporter des réacteurs nucléaires», a-t-il dit sur son compte Twitter.

Le pirate informatique n'a pas précisé le montant qu'il voulait mais a dit que la Corée du Sud finira par perdre beaucoup plus si elle tente d'économiser des centaines de millions de dollars.

Des responsables de Korea Hydro & Nuclear Power Co. (KHNP) ont déclaré n'avoir pas encore pu déterminer la nature des documents dévoilés car le protocole de sécurité bloquait les téléchargements et l'ouverture des fichiers. Il s'agit de la sixième menace de ce genre depuis le 15 décembre dernier.

«Depuis que le soi-disant groupe antinucléaire a fait sa cinquième annonce le 23 décembre, aucune attaque informatique ou fuite d'information n'a eu lieu. Les documents publiés aujourd'hui semblent avoir été obtenus bien avant (le 23 décembre)», a déclaré l'entreprise dans un communiqué.

Jusqu'à présent, le pirate avait demandé à la KHNP de fermer quelques réacteurs nucléaires, menaçant de «semer la destruction» dans les usines nucléaires si ces demandes n'étaient pas respectées avant Noël. Rien ne s'était passé après Noël. La KHNP insiste que le pirate n'a pas pu se procurer d'information confidentielle car son serveur interne a été entièrement isolé depuis le début de l'année dernière.

Le pirate a également félicité dans son dernier message la KHNP pour avoir trouvé 7.000 virus, tout en affirmant que 9.000 autres attendent ses ordres. Les informations divulguées aujourd'hui comprendraient également la transcription d'une conversation téléphonique datant du 1er janvier entre la présidente Park Geun-hye et le secrétaire général des Nations unies Ban Ki-moon.

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 protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire..

Source : <http://french.yonhapnews.co.kr/news/2015/03/12/0200000000AFR20150312002400884.HTML>

Par mathieu@yna.co.kr

En quoi le big data est-il une révolution ? | Le Net Expert Informatique



En quoi le big data est-il une révolution ?

S'il change notre manière de penser – ça a déjà commencé -, le big data transforme également la façon dont nous vivons. Cela touche aussi nos habitudes de travail. La prise de décision se démocratise sur le lieu de travail et beaucoup d'« experts » autoproclamés voient leur expertise remise en cause à la lumière du big data dont les perspectives et les prédictions s'avèrent bien plus exactes.

Viktor Mayer-Schönberger est Autrichien et professeur de gouvernance et de régulation d'Internet au sein de l'Oxford Internet Institute de l'université d'Oxford (Royaume-Uni). Ses recherches portent sur le rôle de l'information dans l'économie en réseau, la confidentialité des données et le big data. Il est l'auteur d'une centaine d'articles et de plusieurs livres qui reçurent différentes distinctions dont Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, 2011 ; avec Kenneth Cukier et Big data : La révolution des données est en marche, Robert Laffont, 2014.

En quoi le big data est-il une révolution ?

Viktor Mayer-Schönberger : le big data est une révolution dans la manière dont nous autres, humains, comprenons et donnons du sens à la réalité qui nous entoure. Dans le passé, à cause des contraintes de collecte et d'analyse des données, nous avons dû étudier de petits sous-ensembles, des échantillons de réalité ; puis, extrapoler l'ensemble à « tout », en espérant que ce « tout » fonctionne identiquement à l'échantillon. Mais, cela nous limitait à l'utilisation d'un certain nombre de méthodologies, demandait beaucoup de soin quant à l'échantillonnage, imposait de savoir à quelle question l'on souhaitait répondre avant de collecter les données et ne nous permettait pas de nous centrer sur des détails.

De plus, nous nous concentrons sur la qualité de la donnée plutôt que sur sa taille. Notre capacité à collecter et analyser un grand nombre de données évolue et nous devenons capables de discerner la réalité « à l'échelle », dans toute sa complexité et son dynamisme. Dans un sens, ce mouvement ressemble au passage des Newtoniens vers le monde einsteinien de la gravité – une transformation de la façon dont nous donnons du sens au monde qui nous entoure. Et cette révolution touche tous les aspects de la vie, de la société et tous les secteurs de notre économie : la politique et la citoyenneté via les plateformes open data (des plateformes de données ouvertes) ; l'urbanisation et l'énergie à travers différents capteurs connectés ; le e-business grâce à l'accès à un nombre croissant de données sur ses consommateurs.



Regroupées massivement, les données numériques peuvent être décryptées pour mieux comprendre le monde qui nous entoure. © R2hox, Flickr, CC by-sa 2.0

Pouvons-nous prévoir le futur avec ces data ?

Dans une certaine mesure, on peut parler de prédictions. Nous l'avons déjà fait auparavant, nous le faisons aujourd'hui en extrapolant le passé ou le présent vers le futur. Cela fonctionne bien si les choses ne changent pas radicalement. Même si ces attentes envers les data tendent à nous dire le contraire, l'individu ne change pas si facilement.

Y a-t-il une limite à la quantité de données que l'on peut créer ?

Non, pour l'instant, aucune limite en vue. Bien sûr, il existe une barrière physique quant à la quantité d'informations qui peut être stockée dans l'univers. Mais cette barrière représente un ordre de grandeur tellement plus grand que ce que nous recueillons et analysons actuellement, qu'elle offre une perspective très importante de croissance. De plus, la chute des coûts de collecte et de stockage associée à de meilleurs outils analytiques rend le big data de moins en moins cher et de plus en plus simple d'usage.

Qu'est-ce qu'un « algorithmiste » et un data scientist ?

Les data scientists – parfois appelés quants (abréviation de quantitative analyst) – font de l'analyse quantitative. Les « algorithmistes » sont des quants qui ont rejoint une profession spécialisée et agissent comme des audits indépendants d'analyse des big data. La relation entre les data scientists et les « algorithmistes », c'est un peu comme avoir étudié le droit et être avocat ou notaire.



Le développement du big data a permis l'analyse de données massives. © Domaine public

Quelles nouvelles compétences demande le big data ?

Le big data nécessite des capacités de collecte et de mutualisation des données (par exemple, à travers de nouveaux capteurs, en les récupérant sur Internet ou en ciblant la valeur dans des données possédées par d'autres, mais pouvant être mises sous licence) ; des compétences d'analyse des données (bien au-delà de la simple statistique) et de compréhension des limites de ces analyses. Ces nouvelles compétences sont déjà enseignées, partout dans le monde, dans des programmes d'études universitaires de pointe qui comportent également une formation pour les spécialistes de l'analyse quantitative.

Quelle est la valeur de ces data ?

Auparavant, la valeur de la data était limitée à l'objectif pour lequel elle avait été collectée. Dans le futur, cette valeur résidera dans les utilisations et réutilisations qui pourront être faites de ces données, même si cela n'était pas apparent au moment de leur collecte. La valeur de la donnée augmente donc avec notre capacité à extraire cette valeur.

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 protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.futura-sciences.com/magazines/high-tech/infos/dossiers/d/high-tech-big-data-boom-donnees-numeriques-1936/page/2/>

Comment se passe un contrôle de la CNIL et comment s'y préparer ?

17



Aucun organisme public ou privé n'est à l'abri d'un contrôle de la CNIL. Il est donc important de se tenir prêt. Pour ce faire, la préparation et la sensibilisation des différents acteurs sont essentielles. Le CIL a bien évidemment une place prépondérante dans ce processus, que ce soit en amont, pendant ou après. Thierry Ramard, Président d'Ageris Group, rappelle les bonnes pratiques pour se mettre en conformité avec la législation et se préparer au mieux à un éventuel contrôle, à l'occasion de 9ème Université des CIL de l'AFCDP.

Les missions de contrôle de la CNIL s'inscrivent dans le cadre d'un programme annuel adopté en séance plénière. Ce programme est élaboré en fonction des thèmes d'actualité et des grandes problématiques dont la CNIL est saisie. Cela représente près de 2/3 des contrôles. Ceux-ci peuvent également être décidés en réponse à des besoins ponctuels, dans le cadre de l'instruction de plaintes, ou de demandes de conseil (environ 1/3 des contrôles).

Selon le rapport d'activité 2013 de la CNIL :

Elle a reçu 5 638 plaintes au cours de l'année 2013 : dans 99% des cas, l'intervention de la CNIL s'est traduite par une suite favorable pour le demandeur ;

414 contrôles ont été réalisés, dont 33% étaient issus de plaintes. 280 contrôles ont concerné des traitements relevant directement de la Loi Informatique et Libertés, et 134 des dispositifs de vidéoprotection/vidéosurveillance. La majorité des contrôles ont été effectués dans le domaine du commerce (117), de la santé et du social (73). 89% des organismes contrôlés se sont mis en conformité après échanges de courriers ;

57 mises en demeure ont été adoptées : 88% d'entre elles font suite à un contrôle, 12% sont directement issues de plaintes sans contrôle sur place. 86% de ces organismes mis en demeure en 2013 se sont mis en conformité ;

14 dossiers ont fait l'objet d'une procédure de sanction.

Contrôle de la CNIL : avant, pendant, après

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source

<http://www.globalsecuritymag.fr/AFCDP-Comment-se-preparer-a-un,20150130,50435.html>

Colloque « Innovation et cybercriminalité : l'Europe face aux défis de la transformation numérique » | Le Net Expert Informatique

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>Colloque à Montpellier « Innovation et cybercriminalité : l'Europe face aux défis de la transformation numérique »</p>
---	---

Programme du Mercredi 8 avril 2015

13:30-14h Accueil des participants

14h:00 Ouverture du colloque :

Philippe Augé, Président de l'Université de Montpellier
Marie-Elisabeth André, Doyen de la Faculté de Droit et Science politique de Montpellier
Adel Jomni, Enseignant-chercheur, Université de Montpellier
Michal Choras, Représentant du projet européen CAMINO
Akghar Babak, Représentant du projet européen COURAGE

14h30 Session 1: Innovations numériques, Cybercriminalité et Cyber-terrorisme : Enjeux et défis : quelles stratégies ? :

Lord Carlile of Berriew, Membre du Parlement du Royaume-Uni,
Général Marc Watin-Aougouard, Directeur du centre de recherche de l'Ecole des Officiers de la Gendarmerie Nationale (EOGN)
Andy Archibald, Directeur adjoint de l'unité nationale cybercriminalité de l'Agence Nationale de la Criminalité du Royaume-Uni
Marco Lozano, Représentant INCIBE (Instituto Nacional de Ciberseguridad de España)

16h:00 Pause

16h:15 Session 2: Les menaces cybernétiques : Analyse des risques et des stratégies? :

Président de session : Cormac Callanan, Expert auprès du Conseil de l'Europe, CEO, Aconite, Irlande
– Etat des lieux des cyber menaces – Jean-Dominique Nollet, Directeur de l'unité d'investigation et recherche (European Cybercrime Centre (EC3-Europol))
– L'investigation et la coopération entre les organisations internationales (Interpol, Europol,..) – Valérie Maldonado, Directrice de l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC)
– Analyse des réseaux sociaux et sécurité nationale – Thomas Delavallade, THALES
– Comment améliorer la résilience face à la cybercriminalité et au cyber-terrorisme (Projet Européen CAMINO – FP7) – Michal Choras, Professeur, Coordinator du projet FP7-CAMINO, ITTI, Pologne

Programme du Jeudi 9 avril 2015

9h:00 Session 3: Enjeux et risques liés au développement des monnaies virtuelles

Président de session : Daniel Guinier, Expert en cybercriminalité, Cour Pénale Internationale de La Haye
– Flux illicites et monnaies virtuelles – Myriam Quémener, Magistrate, Cour d'appel de Versailles
– Monnaie virtuelle et crypto monnaie : quels enjeux et réponses réglementaires? Quelles préconisations pour les utilisateurs et les entreprises? – Cathie-Rosalie Joly, Avocate
– Paiements 2.0: nouveaux défis de sécurité et rôle de l'Autorité Bancaire Européenne – Geoffroy Goffinet, European Banking Authority (EBA)- Bruxelles

10h:15 Pause

10h:30 Session 4: Big data, Internet des objets, Cybersécurité et protection de la vie privée

Président de session : Christian Aghroum, Membre CDSE, Expert en Cybersécurité
– Big Data et sécurité : le pouvoir de l'anticipation au service de la cybersécurité – Adel Jomni, Enseignant-chercheur, Université de Montpellier
– Le droit est-il un frein pour le développement du Big Data ? – Francesca Bosco, Chef de projet UNICRI (United Nations Interregional Crime and Justice Research Institute); Giuseppe Vaciano, Cybercrime Institute, Germany
– Objets connectés et santé : l'innovation au service ou au détriment du citoyen? – Corinne Thierache, Avocate
– Le Big Data : un déclencheur de changement des règles juridiques – Fraser Sampson, Responsable de l'office des crimes – West Yorkshire Police

13h:00 Pause déjeuner

14h:00 Session 5: Projets européens, coopération internationale, recherche et formation dans le domaine de la lutte contre la Cybercriminalité et le Cyberterrorisme

Président de session : – Nigel Jones, Directeur du Centre for Cybercrime Forensics, Université de Canterbury
– Défis majeurs de la recherche dans le domaine de la cybercriminalité et le cyber terrorisme – Akghar Babak, Projet Européen COURAGE
– Nouvelles approches de la protection des données et Cryptographie -Projet ENISA (European Union Agency for Network and Information Security) – María Pilar Torres Bruna, Responsable Cybersécurité chez Everis, Espagne
– Nouvelles méthodes d'investigation et de formation forensique dans un environnement virtuel (cloud) (projet D-FET) – Adrian Smalesn Researcher, Université Napier d'Edimbourg
– La coopération internationale pour renforcer les capacités de protection des infrastructures d'information critiques 2015-2020 (CIIP) – Jean-Christophe Letoquin, Expert auprès du Conseil de l'Europe, Président de SOCOGI
– Coopération internationale en matière de formation cyber (enjeux et rôles des partenaires) ? – Yves Vandermeer, Federal Computer Crime Unit, Belgique E.C.T.E.G Chair (Europol)

16h:00 Fin du colloque

Emportez le programme avec vous ! Téléchargez le PDF

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 protection juridique du chef d'entreprise.
Contactez-nous

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

La justice néerlandaise annule une loi sur les données personnelles | Le Net Expert Informatique



La justice néerlandaise annule une loi sur les données personnelles

La justice néerlandaise a annulé mercredi une loi exigeant le stockage de données personnelles, assurant que bien qu'utile à la lutte contre le crime, le texte violait la vie privée des utilisateurs des réseaux téléphoniques et d'internet.

« Les juges ont estimé que le stockage de données était nécessaire et efficace pour combattre le crime, mais la législation néerlandaise est contraire aux droits des personnes à une vie privée et à la protection de leurs données personnelles », a indiqué le tribunal de La Haye dans un communiqué.

« La loi est donc contraire à la Charte des droits fondamentaux de l'Union européenne », a ajouté le tribunal.

Sept organisations, dont l'organisation de défense de la vie privée Privacy First et l'Association néerlandaise des Journalistes, avaient entamé une action contre l'État le mois dernier.

Cette décision des juges intervient environ un an après une décision de la justice européenne, qui avait imposé en avril 2014 une révision de la législation sur la conservation des données personnelles, la jugeant « disproportionnée » malgré son utilité dans la lutte contre le terrorisme.

La directive en question datait de 2006 et exigeait des opérateurs de télécoms et des fournisseurs d'accès internet de stocker les données des communications téléphoniques ou de courriels pendant six mois à deux ans.

Étaient donc conservées les métadonnées desdites communications, comme l'heure, la date, la durée et la destination, mais pas leur teneur.

Ces données pouvaient ensuite être consultées par les services de renseignement ou la police.

« Les droits à une vie privée des citoyens néerlandais ont été violés en masse par cette surveillance », a affirmé Vincent Boehre, le directeur des opérations de Privacy First, cité dans un communiqué publié sur le site internet de l'organisation.

Privacy First « lutte pour une société dans laquelle des civils innocents ne doivent pas se sentir comme s'ils étaient constamment surveillés », a-t-il ajouté, soulignant que ce jugement est « une étape importante dans cette direction ».

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 protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire..

Source

<http://www.leparisien.fr/high-tech/la-justice-neerlandaise-annule-une-loi-sur-les-donnees-personnelles-11-03-2015-4595081.php>

Accord pour faciliter les plaintes transfrontalières | Le Net Expert Informatique



Accord pour
faciliter les
plaintes
transfrontalières

Les Etats membres de l'Union européenne se sont accordés ce vendredi à Bruxelles sur le principe de permettre aux entreprises et aux citoyens le dépôt, au sein de leur Etat national, d'une plainte en matière de protection de la vie privée contre une entreprise du web établie dans un autre Etat.

Ce guichet unique («one-stop-shop») serait compétent pour veiller à l'application des règles pour les transferts transfrontaliers de données personnelles collectées dans plusieurs pays de l'UE par des entreprises ou des plate-formes internet comme Amazon, Google, Facebook.

Les plaignants auront la possibilité de saisir leurs autorités nationales, comme la Commission de la protection de la vie privée en Belgique, en cas de litige.

Le but est d'obtenir une procédure plus rapide, des coûts et une charge administrative moindres ainsi qu'une sécurité juridique accrue.

Le secrétaire d'Etat belge en charge de la protection de la vie privée, Bart Tommelein, ne voit que des avantages au principe du guichet unique, mais reconnaît sa complexité. «Nous devons activer ce système avant de voir par la suite comment l'améliorer et le simplifier», a-t-il commenté.

Un accord global sur la législation sur la protection des données personnelles est toutefois encore loin d'être définitif.

Les ministres européens de la Justice ont donc décidé de se réunir en «conclave» le 15 juin à Luxembourg afin de conclure un accord.

Les discussions sont engagées depuis février 2012, mais elles ont longtemps piétiné. Onze chapitres sont ouverts, et six ont fait l'objet d'un accord de principe, dont celui portant sur la création d'un «guichet unique».

Sur les cinq restant en discussion, on relève celui concernant les droits des personnes, avec le droit d'accès aux données collectées, le droit de les faire rectifier et le droit à l'oubli avec la possibilité «de faire effacer les informations mises en ligne avec insouciance par les mineurs».

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 protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : http://www.lavenir.net/cnt/dmf20150313_00616117

La CIA aurait cherché à percer la sécurité de l'iPhone | Le Net Expert Informatique



La #CIA aurait cherché à percer la sécurité de l'iPhone

C'est ce que révèlent de nouveaux documents transmis par Edward Snowden, et publiés par le site américain The Intercept.

Nouvelles révélations de nos confrères de The Intercept sur les pratiques d'espionnage des Etats-Unis. S'appuyant une nouvelle fois sur des documents transmis par Edward Snowden, le site américain fait état de l'existence d'une mission secrète de la CIA, initiée en 2006, visant à casser le système de chiffrement des terminaux iOS, iPhone et iPad.

L'agence américaine aurait notamment mis au point une version modifiée de l'environnement de développement Xcode : l'IDE conçu par Apple à destination des développeurs souhaitant créer des « apps natives » pour iOS. Cette édition modifiée permettrait d'aboutir à des applications dont les données seraient accessibles à la CIA, ces applications pouvant aussi servir de cheval de Troie sur le terminal – en désactivant ses fonctions de sécurité.

En revanche, aucune des pièces publiées par The Intercept ne tend à indiquer que l'opération a été un succès.

Les nouveaux documents d'Edward Snowden évoquent par ailleurs la tenu d'un événement secret survenu en 2012, le jamboree, lors duquel CIA et #NSA auraient partagé des informations. Le projet de hacking d'iOS y aurait notamment été présenté, lors d'une conférence titrée « Strawhorse: Attacking the MacOS and iOS Software Development ».

Expert Informatique 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 protection juridique du chef d'entreprise. Contactez-nous

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

S o u r c e

http://www.journaldunet.com/solutions/dsi/la-cia-aurait-cherche-a-casser-la-securite-de-l-iphone-0315.shtml?een=4a4b0e45c54d9fed8fc26819a6b6f84f&utm_source=greenarrow&utm_medium=mail&utm_campaign=m149_6outilsdanaly