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

| | |
|---|---|
|  | Skype sur écoute : un amendement de la loi Macron relance le débat |

**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.

---



---

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

# 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…

Source : 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=ml49_6outilsdanalys

# Un radar pour détecter les petits drones | Le Net Expert

# Informatique

## Un radar pour détecter les petits drones

**La détection de drones de moins d'un mètre d'envergure est un sérieux défi technologique. Tecknisolar, une société basée à Saint-Malo, a développé un radar portable et autonome, « parfaitement adapté à la surveillance des zones sensibles ».**

Les récents survols de villes, de centrales nucléaires ou de terrains militaires comme l'Ile-Longue par des drones ont-ils dopé la vente de votre radar spécialisé dans la détection de petites cibles ?
Pascal Barguirdjian : Non, pas plus que cela. Les autorités militaires font la sourde oreille. Pourtant, notre radar fonctionne et a fait ses preuves auprès des gendarmes et douaniers d'Outremer (Cegom).

**Quand l'avez-vous sorti et comment marche-t-il ?**
Nous l'avons développé à la demande d'un général de gendarmerie alors patron du Cegom, en 2007. Nous avons livré quelques-uns de ces radars (100.000 euros pièce) capables de détecter des intrusions d'embarcations dans des zones maritimes sensibles. Ce système composé d'une antenne, d'un écran et de panneaux solaires pour une alimentation autonome est également adapté aux petits engins volants.

**Quel est le rayon d'action de votre système ?**
Il est capable de détecter des embarcations dans un rayon de 15 km comme des engins volants d'un peu plus d'un mètre d'envergure jusqu'à 2 km.

**Et les plus petits, ceux que l'on soupçonne de survoler centrales nucléaires et zones militaires ?**
Leur surface de réflexion est encore trop faible mais notre radar peut relever des échos dans un rayon de 500 m. Toute la difficulté réside dans la détection d'un engin de moins d'un mètre évoluant au ras du sol.

**Les laboratoires militaires cherchent à détecter des engins de 50 cm d'envergure, qu'en pensez-vous ?**
C'est très difficile, voire impossible.

**Quelle est la parade après avoir détecté un drone ?**
On peut le suivre à la trace ou notamment déterminer un cap de fuite pour tenter de le retrouver. Le plus efficace semble le brouillage de sa fréquence GPS pour le faire s'écraser au sol.

**Quel est le risque d'un survol de drone de petite taille, à la charge utile forcément limitée ?**
Ces drones peuvent être mis en oeuvre par des services secrets qui réalisent la collecte d'informations. L'acte terroriste avec une flotte de drones décollant sur une cible et transportant individuellement quelques centaines de grammes de puissant explosif est à craindre. La menace la plus sérieuse étant, selon moi, l'attaque bactériologique au-dessus d'une ville ou d'un stade de football plein à craquer.

---

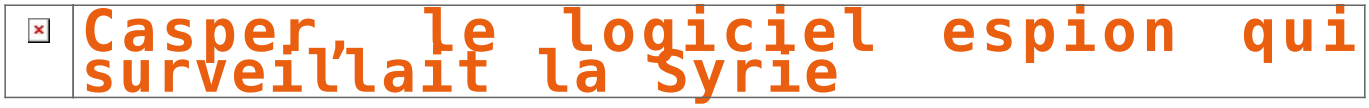


---

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

Source : http://www.letelegramme.fr/economie/drones-un-radar-imagine-a-saint-malo-14-03-2015-10557015.php
www.tecknisolar.com

# Casper, le logiciel espion qui surveillait la Syrie | Le Net Expert Informatique



**Un chercheur en informatique a découvert un nouveau programme espion, qu'il attribue aux mêmes développeurs que le programme Babar, pour lequel la France est soupçonnée.**

Les développeurs des programmes espion Babar et Evil Bunny, que le Canada soupçonne être les services de renseignement français, ont créé un troisième programme espion qui ciblait la Syrie.
Pour rappel, Le programme espion Babar a un « grand frère » : Evil Bunny
C'est la conclusion à laquelle aboutit Joan Calvet, un expert de l'entreprise de sécurité informatique ESET dans un rapport qui doit être publié jeudi 5 mars. Il a pu mettre la main sur un exemplaire de ce nouveau programme, dont le nom que lui ont donné ses créateurs reprend à nouveau celui d'un célèbre dessin animé. Cette fois-ci, les développeurs ont baptisé leur création Casper.

**Une dizaine de personnes visées en Syrie**
Ce logiciel a été retrouvé sur les ordinateurs d'une dizaine de personnes, toutes situées en Syrie. Il n'est pas exclu que ce programme ait été mis en œuvre ailleurs. Il a aussi été utilisé très récemment – contrairement à Babar – et faisait partie d'une opération bien précise : il a été actif en Syrie seulement quelques jours, entre le 9 et le 16 avril 2014.
La trace de ce programme a été retrouvée sur un site officiel du gouvernement syrien, celui d'une commission créée en 2011 sous l'égide du ministère de la réconciliation nationale afin que les Syriens victimes de destructions lors de la guerre civile puissent porter réclamation.

**Un programme de reconnaissance**
A l'inverse de Babar, Casper ne capture pas d'informations directement : c'est un programme de reconnaissance. Lorsqu'il pénètre dans un ordinateur, il en établit un descriptif précis – langue utilisée, programmes installés, logiciels antivirus configurés – avant de le faire parvenir à ses commanditaires. Ensuite, ces derniers décident si la cible est réellement digne d'intérêt.
Le deuxième stade est vraisemblablement celui de l'envoi d'un autre programme espion capable, lui, d'intercepter des informations. Casper prévoit d'ailleurs ce cas de figure : il peut lui être ajouté des modules complémentaires. Cette technique est de plus en plus courante dans les attaques étatiques sophistiquées.

**Un programme fantomatique et complexe, une « partie d'échecs » avec les logiciels antivirus.**
Ce programme espion au nom de fantôme porte bien son nom, tant il est difficile à détecter. Lorsqu'il atterrit sur un ordinateur, Casper s'adonne à une « partie d'échecs » avec les logiciels antivirus : il analyse très finement lesquels sont présents sur la machine et adapte son mode d'infection. Dans certains cas, il peut tout bonnement s'autodétruire lorsqu'il estime que les risques sont trop grands. « On voit rarement ce niveau de précision dans l'évitement des antivirus chez les programmes espion », note Joan Calvet, signe là encore d'une grande sophistication.
« Casper est tellement furtif et sous le radar des entreprises de sécurité, qu'on ne retrouve sa trace qu'épisodiquement pour le moment. J'espère qu'en publiant ces informations, d'autres chercheurs vont pouvoir amener leur pièce au puzzle ! », explique aussi M. Calvet.
Signe supplémentaire de sa complexité et de la motivation des attaquants, il utilise une faille dite « 0-Day », c'est-à-dire une vulnérabilité inconnue. Ce type de vulnérabilité, inédite donc invisible pour les antivirus, intéresse de près les chercheurs en sécurité informatique. Utiliser une telle faille, c'est prendre le risque de l'exposer en plein jour et de la voir rapidement corrigée.

**Les mêmes auteurs que Babar**
Pour Joan Calvet, il n'y a guère de doute. Casper est l'œuvre des développeurs qui ont créé Babar et Evil Bunny. Outre des portions du code rigoureusement identiques entre ces programmes, il leur a trouvé de nombreux points communs, notamment dans leur manière de se cacher ou de détecter les antivirus.
« Toutes les fonctionnalités communes nous font dire avec un haut degré de certitude que Bunny, Babar et Casper ont été développés par la même organisation », écrit Joan Calvet.

**Un Etat à la manœuvre ?**
Casper, comme Babar, n'est pas un programme d'espionnage massif, comme certains dispositifs révélés par les documents d'Edward Snowden. Il s'agit d'outils de haut niveau destinés à obtenir des informations précises sur des cibles déterminées. Selon M. Calvet, « le ciblage précis d'individus en Syrie montre un intérêt géopolitique probable » :
« Non seulement Casper est bien développé, mais en plus ses auteurs semblent bien comprendre comment nous – les chercheurs en sécurité – travaillons, et ils ont fait en sorte de rendre notre tâche difficile. En regardant rapidement le programme, on peut avoir l'impression d'avoir sous les yeux un logiciel malveillant banal, sans se douter de toute la machinerie de reconnaissance contenue dans Casper. Je dirais donc que Casper a été développé par une équipe de professionnels, soucieuse de faire un logiciel malveillant discret. Ce "professionnalisme" peut tout à fait correspondre à une entité étatique. »

**France : quelle implication ?**
En 2014, Le Monde révélait sur la base de documents fournis par Edward Snowden que les services de renseignement canadiens soupçonnaient la France d'avoir développé un programme espion nommé Babar.
Rappel : Quand les Canadiens partent en chasse de « Babar »
Il y a quelques semaines, deux chercheurs en informatique révélaient davantage d'informations sur Babar et dévoilaient du même coup l'existence d'Evil Bunny, le « grand frère », moins évolué, de Babar, développé par la même organisation.
Pas de trace nouvelle d'une implication hexagonale dans Casper. La France, qui à ce stade n'est que soupçonnée par les services de renseignement canadiens d'être derrière Babar, et donc derrière Casper, s'est dotée, comme les autres grandes puissances militaires mondiales, de capacités offensives sur Internet, confiées à l'armée et aux services extérieurs, la DGSE. Les autorités refusent de s'exprimer sur ce sujet extrêmement sensible, couvert par le plus haut niveau du secret-défense. Récemment, une vidéo réalisée par l'armée française rompait légèrement avec ce mutisme en vantant ses capacités d'« attaque » et « destruction » dans ce « combat numérique ».

---

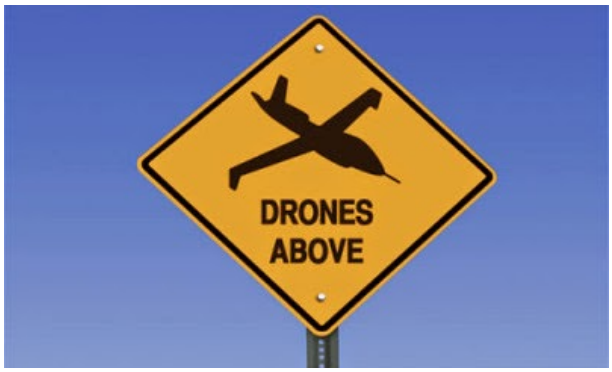


---

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

Source : http://www.lemonde.fr/pixels/article/2015/03/05/casper-le-logiciel-espion-cousin-de-babar-qui-surveillait-la-syrie_4586723_4408996.html
Par Martin Untersinger

# Réglementation des drones et droit des robots | Le Net Expert Informatique




source : http://live.orange.com/drones-parrot-amazon-zephyr/

Réglementation des drones et #droit des robots

**Le survol des drones au dessus des centrales nucléaires [1] ainsi que d'autres sites sensibles et parisiens [2]  représente une menace face à laquelle les réponses, notamment réglementaires, semblent encore insuffisantes.**

En effet, la détection par radar militaire mais également l'interception de ces engins volants se révèlent difficiles de par la furtivité des drones et l'incapacité actuelle des autorités à les tracer et à les écarter.

Au niveau réglementaire, l'utilisation des drones ou plus exactement d' « aéronefs qui circulent sans monde à bord » civils, à distinguer des drones militaires, est encadrée par deux arrêtés d'avril 2012 [3], un arrêté relatif aux conditions de navigabilité et de télépilotage et un autre relatif aux exigences liées à l'espace aérien.

**Le principe est le suivant :**
sauf autorisation particulière, les drones doivent survoler un espace bien précis délimité en volume et en temps, en dehors de toute zone peuplée. De plus, en fonction de deux catégories de critères (finalité d'utilisation et poids du drone), des règles particulières s'appliquent. Ainsi, les drones civils professionnels utilisés par exemple par les agriculteurs ou les photographes doivent  notamment se faire connaître auprès des autorités.
Concernant l'utilisation de drone de loisirs qui est en vente libre, il faut également respecter des règles spécifiques qui sont rappelées dans une notice rédigée par la Direction Générale de l'Aviation Civile (DGAC) en décembre 2014 [4] et qui interdisent notamment le vol de nuit, le survol des sites sensibles ainsi que de l'espace public en agglomération.
Au final, la violation des conditions d'utilisation des drones est passible d'un an d'emprisonnement et de 75000 euros d'amende en vertu de l'article L.6232-4 du code des transports.
Autre point d'importance à souligner, même si la prise de vue aérienne est réglementée par l'article D. 133-10 du code de l'aviation civile, il n'en demeure pas moins que la captation et l'enregistrement d'images relatives aux personnes relèvent également de la loi « Informatique et Libertés »[5].
En effet, il est important de souligner également le risque de collecte de données à caractère personnel par les drones. Un facile parallèle peut être établi entre le survol des drones et le passage dans nos rues des « Google cars ».  La CNIL avait constaté lors de contrôles effectués fin 2009 et début 2010 que la société Google, via le déploiement de véhicules enregistrant des vues panoramiques des lieux parcourus, récoltait, en plus de photographies, des données transitant par les réseaux sans fil Wi-Fi de particuliers, et ce à l'insu des personnes concernées. Cette collecte déloyale de très nombreux points d'accès Wi-Fi  constitue un réel manquement à la loi « Informatique et Libertés ».
Concernant les drones, il faudra donc s'attacher à vérifier qu'ils ne récupèrent pas également des données à caractère personnelle de façon illégale. En effet, les drones sont des machines qui peuvent embarquer une quantité importante de capteurs divers et variés tels un appareil photo, une caméra ou un dispositif de géolocalisation permettant de collecter et diffuser des données à caractère personnel avec pour conséquence l'atteinte manifeste à la vie privée des individus.
Consciente de ces enjeux depuis 2012, la CNIL, en liaison avec le Groupe des 29 CNIL européennes (G29) réfléchit activement à l'amélioration de la réglementation à ce sujet.

Au final, la réglementation relative aux drones qui, d'une part, a le mérite d'exister et, d'autre part, est relativement souple et adaptable en prévoyant plusieurs scénarii spécifiques, apparaît même novatrice au niveau international. Les Etats Unis par l'intermédiaire de la Federal Aviation Association (FAA) n'ont dévoilé que le 15 février 2015 et pour la première fois des recommandations pour encadrer l'utilisation des drones civils commerciaux sur le sol américain [6].
Toutefois, la DGAC a prévu quand même de réviser prochainement la réglementation des drones afin de mieux prendre en compte la massification de l'utilisation de drones civils. Cette révision devra si possible prendre en compte une future réglementation européenne à ce sujet.

Plus largement, ce focus juridique sur les drones peut élargir son horizon en s'intéressant à la problématique du droit des robots qui, au regard de la vitesse de création des inventions technologiques, constitue indéniablement un des enjeux majeurs juridiques mais également éthiques des années à venir.
Certes pour les objets connectés, les enjeux juridiques ont déjà été identifiés mais il semble qu'il faille pousser le cadre juridique plus loin pour les futures générations de robot doté d'une certaine forme d'intelligence artificielle.
La vente du robot, comme tout bien, entraine pour le vendeur une obligation de garantie et engage sa responsabilité délictuelle du fait d'un défaut de sécurité de l'un de ses produits ou services entraînant un dommage à une personne. Cependant, il est probable que l'autonomie des robots grandissante, il faille réfléchir à la responsabilité propre du robot. De prime abord, la responsabilité juridique repose sur la notion de discernement, actuellement les machines restent sous la responsabilité de son gardien soit de l'usager ou encore de son fabricant par le biais de la responsabilité des produits défectueux.
Il est possible que, dans un futur plus ou moins proche, le législateur décide de mettre en place une personnalité juridique spécifique du robot. Cette dernière, se distinguant du régime juridique lié aux animaux et des biens, devra être encadrée afin de prévoir la sécurité des utilisateurs mais également la sécurité du robot lui-même. Pour commencer, il pourrait même s'agir de la reprise des trois règles de la robotique édictée par Isaac Asimov [7]!

[1] Dix-sept centrales nucléaires sur les dix-neuf que compte le parc français ont été survolées par des drones depuis début octobre. Six l'ont été simultanément dans la nuit du 31 octobre.
[2] http://www.liberation.fr/societe/2015/02/24/paris-survole-par-des-ovnis_1209273
[3]Les arrêtés du 11 avril 2012 relatifs d'une part à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord et d'autre part à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent constituent le socle réglementaire d'utilisation des drones civils.
[4] Règles d'usage d'un drone de loisir :  http://www.developpement-durable.gouv.fr/IMG/pdf/Drone-_Notice_securite-2.pdf
[5] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.
[6] « Drones civils – les Etats-Unis avancent sur leur législation : les différences avec le modèle français  » par Emmanuel de Maistre, président de Redbird : http://www.infodsi.com/articles/154099/drones-civils-etats-unis-avancent-legislation-differences-modele-francais-emmanuel-maistre-president-redbird.html?key=a0a42d0bc78aa63d
[7] http://nte.mines-albi.fr/SystemiqueSudoku/co/v_regle_vie_Azimov.html

---



---

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

Source : http://securitedessystemesjuridiques.blogspot.fr/2015/03/reglementation-des-drones-et-droit-des.html

---

# Écoute téléphonique des

# salariés : création de la norme simplifiée n°57 par la CNIL | Le Net Expert Informatique

## Écoute téléphonique des salariés : création de la norme simplifiée n°57 par la CNIL

**La CNIL, le 27 novembre 2014, a offert aux entreprises une nouvelle norme simplifiée pour leur permettre de déclarer rapidement et facilement les traitements de données relatifs à l'écoute et à l'enregistrement des conversations téléphoniques sur le lieu de travail. Il s'agit de la norme simplifiée n°57.**

Puisque l'informatique est partie inhérente de l'entreprise il revient à l'employeur de prendre les mesures adéquates et légales pour mettre en œuvre ses traitements de données de salariés.

Or, tout traitement de données à caractère personnel doit faire l'objet d'une déclaration préalable à la CNIL. Il s'agit par exemple du traitement de gestion des badges d'accès aux locaux, de la messagerie électronique, le cas échéant, la vidéosurveillance ou encore tout traitement ayant pour finalité le contrôle de l'activité des salariés. C'est donc bien le cas pour l'écoute des salariés.

A cette fin, l'entreprise doit adhérer à la norme simplifiée n°57 pour tout traitement de données à caractère personnel destinés à l'écoute et l'enregistrement ponctuel des conversations téléphoniques sur le lieu de travail à des fins de formation et évaluation des employés ainsi que l'amélioration de la qualité du service fourni.

Attention il est impératif de respecter le contenu de la norme. A défaut la déclaration à la CNIL ne serait pas prise en compte. Il faut donc relire la norme simplifiée n°57 et mettre à jour ses processus internes afin de la respecter, par exemple pour les durées de conservation.

Cette déclaration à la CNIL n'est pas la seule formalité à respecter, en effet comme toute modification des conditions de travail, la mise en place d'un dispositif d'écoute des salariés doit être soumise à l'information et la consultation des instances représentatives du personnel.

La mise en place de telles écoutes permet à l'employeur de collecter notamment des données sur l'activité des salariés.

A défaut de déclaration à la CNIL, il y a un risque important pour l'employeur qui réside dans l'impossibilité d'utiliser les données collectées par l'entreprise dans le cadre d'une procédure de licenciement d'un salarié.

A NOTER : la jurisprudence de la Chambre sociale de la Cour de cassation du 8 octobre 2014 rappelle que la déclaration de ces dispositifs de collecte de données des salariés doit être préalable à leur mise en œuvre. A défaut, tout licenciement basé sur des preuves collectées par ce dispositif d'écoute serait jugé sans cause réelle et sérieuse pour illicéité de la preuve.

---



---

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

Source :
http://www.village-justice.com/articles/ecoute-telephonique-des-salaries,19088.html
Par Yaël Cohen-Hadria, Avocat

# Les travel managers doivent-ils craindre Prism ? | Le Net Expert Informatique

Les travel managers doivent-ils craindre Prism ?

**Comment fonctionne Prism ? Quel en est l'intérêt pour les compagnies aériennes ? Celui des entreprises ? Qu'en est-il de la confidentialité ? Telles sont quelques unes des questions qui agitent le monde des travel managers. Éléments de réponse.**

Malgré les petits fours, malgré le poisson et la volaille à la julienne de légumes suivie d'un assortiment de desserts programmé pour coïncider avec le service d'un dernier verre de champagne, le dîner aérien organisé le 10 février dernier dans un chic hôtel parisien par l'AFTM – l'Association française des travel managers, dont c'est un des rendez-vous les plus prisés – en a laissé plus d'un sur sa faim… Pour cause : le thème de cette soirée – débat était « Qu'est-ce que Prism ? ». Une question qui n'avait jamais encore été mise sur la table en France, alors même qu'un nombre croissant d'entreprises se la posent en interne. « De nombreuses interrogations sont restées en suspend », confirme le délégué général de l'association, Thibault Barat.

**« Beaucoup d'incompréhension »**

Sur son site internet, Prism – passé il y a trois ans sous le contrôle du groupe américain Sabre – se définit comme le leader de la data sur les voyages corporate, qu'il collecte et consolide pour les compagnies aériennes. « Il y a beaucoup d'incompréhension sur le sujet », souligne néanmoins Thibault Barat, qui rappelle que Prism a commencé à revenir avec insistance aux oreilles des travel managers français alors que l'affaire Snowden était sur le devant de la scène. Une association sulfureuse qu'une autre coïncidence ne fait rien pour atténuer : Prism est aussi le nom donné à un programme de surveillance électronique américain relevant des activités de la NSA… « Nous ne faisons que gérer de la data », a martelé Herman Mensink, vice-président de Prism pour la zone Europe, Moyen Orient et Afrique. Une vocation d'apparence plutôt bénigne qui comporte toutefois d'importantes zones de gris.

**« Que va-t-on faire de nos données ? »**

« Que va-t-on faire de nos données ? », s'est inquiété un travel manager qui participait à ce dîner débat – et qui a tenu à conserver l'anonymat. A en croire les nombreuses questions qui ont fusé, une fois la présentation de Herman Mensink terminée, la protection de données, parfois hautement stratégiques, s'impose comme le souci majeur des entreprises françaises face à la montée en puissance de Prism. Inquiétude balayée d'un revers de manche par son vice-président EMEA: « La vocation du groupe est de gérer des données ». Comprendre : tout autre aspect du programme relève de la négociation entre les entreprises et les compagnies aériennes.

Une auto-justification qui a surtout pour conséquence de mettre en exergue l'un des points du dispositif Prism jugés problématiques : « Aucun contrat n'unit Prism aux entreprises. Ces dernières ne sont en interaction qu'avec les compagnies aériennes, qui, lorsqu'elles contractualisent avec Prism, leur demandent de communiquer leurs données à Prism, tiers avec qui elles n'ont aucun lien légal ». Moyennant quoi les entreprises ont accès à une tarification avantageuse.

La formule n'est pas sans rappeler l'accord déjà en place entre les travel managers corporate français et Air France. Sauf que là, souligne notre travel manager anonyme, « Rentre dans le process un intervenant extérieur qu'on ne maîtrise absolument pas. Quelle garantie avons-nous vis-à-vis de ses agissements ? Et, en cas de litige, qui tranchera ? » (les donnée collectées en mode cloud par Prism sont stockées, pour une durée d'un an minimum, sur des serveurs situés aux États-Unis).

---

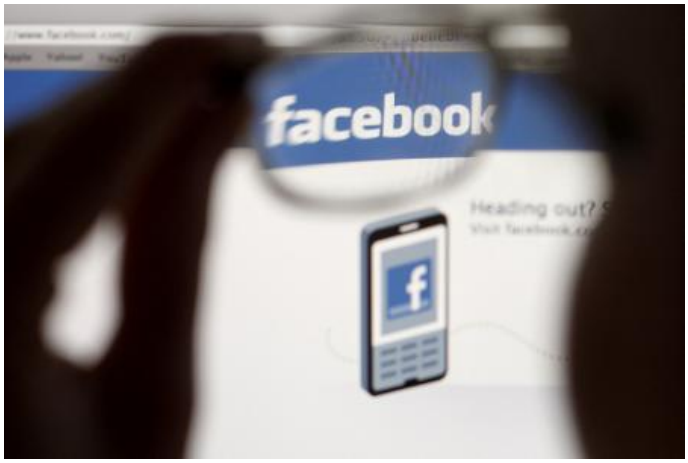


---

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

Source : http://www.decision-achats.fr/Thematique/marches-1036/travel-meetings-10135/Breves/travel-travers-Prism-251605.htm

# Inquiétant: les employés de Facebook n’ont pas besoin de votre mot de passe pour accéder à votre profil | Le Net Expert Informatique

| | |
|---|---|
|  | Inquiétant : les employés de Facebook n’ont pas besoin de votre mot de passe pour accéder à votre profil |

**Voilà une révélation qui ne va pas rassurer alors que la protection des données personnelles sur Internet est une véritable préoccupation des internautes : selon un artiste finlandais, les employés de Facebook ont accès à tous les profils du réseau social… sans mot de passe.**

Le musicien finlandais Paavo Siljamäki était en visite, le 24 février dernier, dans le quartier général de Facebook, à Los Angeles. Il a alors eu droit à une démonstration de l'utilisation du réseau social par des employés du site web. Et ceux-ci ont montré qu'ils pouvaient aller bien plus loin qu'une simple visite de profil.

« Un ingénieur de Facebook s'est connecté directement comme s'il était sous mon nom sur Facebook, et pouvait donc voir tout mon contenu privé sans demander de mot de passe », explique le musicien… sur Facebook. « C'est pourquoi je me demande combien d'employés de Facebook ont la possibilité d'avoir accès à tous les comptes ? Quelles sont les règles sur qui et quand peut-on avoir accès à nos données privées et comment pourrait-on le savoir que quelqu'un y a eu accès ? (Mon compte ne m'a pas indiqué que quelqu'un avait accédé à mon profil) ».
Ces questions, n'importe quel utilisateur de Facebook pourrait se les poser. En cette période trouble durant laquelle de nombreux internautes s'interrogent sur la protection de leurs données personnelles par les grandes compagnies comme Facebook, Google, Apple, Amazon, etc.
Facebook a partiellement répondu aux questions de Paavo Siljamäki sur VentureBeat. Un porte-parole explique ainsi que seuls des employés désignés ont accès « aux informations nécessaires pour faire leur travail », à savoir résoudre des bugs ou répondre aux demandes d'aide. Des équipes de sécurité indépendantes gèrent ensuite les cas considérés comme suspects par des groupes de travail mis en place au sein des équipes de Facebook, et contrôlés, du moins pour l'Europe, par le bureau de la commission irlandaise de protection des données.
VentureBeat confirme donc que Facebook peut avoir accès à tous les profils sans mot de passe, mais seulement si cela est demandé pour les raisons ci-dessus et si vous l'autorisez.

---



---

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

Source : http://www.sudinfo.be/1225989/article/2015-03-02/inquietant-les-employes-de-facebook-n-ont-pas-besoin-de-votre-mot-de-passe-pour

---

# La NSA et sa consœur britannique surveillent aussi les cartes SIM

Crédit : Fotolia

# La NSA et sa consœur britannique surveillent aussi les cartes SIM

**Aucun vecteur informatique ne semble échapper aux radars de l'agence de sécurité américaine. Cette fois, la NSA (et la GCHQ) s'est offert un accès aux clients de 450 opérateurs, via les cartes SIM.**

Une nouvelle révélation sur la NSA démontre, si ce n'était pas déjà suffisant, l'étendue de la portée de l'agence de sécurité américaine. Selon le site The Intercept, l'organisation accompagnée par son homologue britannique, le GCHQ, ont toutes deux pénétré dans les réseaux informatiques du premier fabricant de cartes SIM dans le monde, le franco-néerlandais Gemalto, qui produit plus de deux milliards de cartes par an.

A ce stade, la société ciblée ne peut pas « confirmer ces informations » et souligne qu'elle n'avait « aucune connaissance préalable que ces agences gouvernementales conduisaient cette opération », rejetant donc une quelconque complicité. Gemalto indique prendre cet article « très au sérieux » et met en œuvre « tous les moyens nécessaires pour investiguer et comprendre l'étendue de ces techniques sophistiquées ».
Selon The Intercept, qui se base sur des documents fournis par le lanceur d'alertes Edward Snowden, la NSA et le GCHQ ont mis la main sur des clés de chiffrement après avoir installé un malware sur des ordinateurs de Gemalto. Pour cela, l'agence américaine aurait fait appel à son programme de surveillance XKeyscore, qui lui donne accès aux e-mails, conversations Facebook et historiques Internet, lui aussi mis au jour, en août 2013.
Ces clés, utilisées pour protéger la confidentialité des communications téléphoniques, permettent aux deux organisations d'intercepter les échanges vocaux, les SMS et les données Internet des clients mobiles.

**Les clients de 450 opérateurs écoutés**
En visant Gemalto, les deux consœurs ont pu toucher les clients de 450 opérateurs de téléphonie mobile dans 85 pays. « En possédant ces clés de chiffrement, les agences de renseignement peuvent surveiller les communications mobiles sans demander l'autorisation des opérateurs télécoms ni des gouvernements étrangers », écrit l'auteur de ces révélations. Il ajoute que « c'est aussi un moyen de se passer de mandat, tout en ne laissant aucune trace sur le réseau qui révéleraient que des personnes ont été mises sur écoute ».
La révélation de ce nouvel avatar de la surveillance américaine intervient alors que que le ministre de l'Intérieur, Bernard Cazeneuve, est en déplacement aux États-Unis, où il tente de mobiliser les grands acteurs comme Google et Facebook dans la lutte anti-terroriste sur Internet. S'il leur est demandé une collaboration plus étroite avec le gouvernement sur les enquêtes en cours, et une meilleure réactivité sur la suppression du contenu appelant au terrorisme, rien ne semble empêcher le travail en tâche de fond de la tentaculaire NSA.

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

Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-755133-sim-gemalto.html
Par Thomas Pontiroli

# Géolocalisation : tous traqués ? Emission du 12 février 2015 à voir ou à revoir | Le Net Expert Informatique

## Géolocalisation : tous traqués ? Emission du 12 février 2015 à voir ou à revoir

**Les Français utilisent leur portable près de 170 fois par jour. Mais ils font bien plus que téléphoner. Ils prennent des photos, vont sur les réseaux sociaux, se déplacent… tout en se géolocalisant. Pour Envoyé spécial, une équipe a rencontré plusieurs adeptes de ce procédé.**

Grâce à la puce GPS de leur smartphone, ils peuvent trouver la boulangerie ou le cinéma le plus proche, calculer leur trajet en voiture ou en bus, repérer les embouteillages… Plus surprenant : ils peuvent aussi suivre leurs amis à la trace, draguer des passant(e)s, payer leur prime d'assurance de voiture moins cher et même… gagner de l'argent en faisant leurs courses ! Tout ça grâce à des applications de géolocalisation qui se téléchargent en un clic sur leur téléphone.
Mais à force de dire en permanence où nous sommes, notre portable est devenu un véritable mouchard, capable de nous traquer à notre insu… Une aubaine pour les publicitaires, les géants du net, et même les enseignes – qui peuvent cibler le contenu qu'ils vous envoient.
La géolocalisation est désormais une arme commerciale redoutable. Envoyé spécial a enquêté sur ce phénomène mondial qui menace notre vie privée.

---

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.francetvinfo.fr/replay-magazine/france-2/envoye-special/envoye-special-du-jeudi-12-fevrier-2015_822079.html