

# Le Pentagone visé par une cyber-attaque russe ! | Le Net Expert Informatique



Le Pentagone visé par une cyber-attaque russe !

**Aux alentours du 25 juillet, des pirates informatiques russes ont lancé « une cyber-attaque sophistiquée » contre un système de courriels non confidentiels de l'état-major interarmées au Pentagone, selon des responsables américains ayant requis l'anonymat et cités par la chaîne NBC. Aucune fuite d'informations secrètes n'aurait eu lieu.**

Le système informatique du Pentagone est débranché depuis une quinzaine de jours, l'attaque ayant visé 4 000 civils et militaires qui travaillent pour l'état-major interarmées, précise NBC.

Le Pentagone confirme avoir mis le système hors-circuit pour mener une enquête approfondie.

« Par principe et pour des raisons de sécurité opérationnelle, nous ne commentons pas les cyber-incidents ou attaques contre nos réseaux », a indiqué la lieutenant-colonel Valérie Henderson, l'une des porte-paroles du Pentagone dans un courriel.

Selon NBC, l'attaque était automatisée et a réussi, en moins d'une minute, à amasser et à rediffuser les informations collectées sur Internet. La cyber-attaque a été coordonnée par le biais de comptes cryptés et par les réseaux sociaux, d'après ces responsables américains anonymes. Le gouvernement russe n'a pas été directement accusé d'être à l'origine de l'attaque. Mais au regard de sa sophistication, l'attaque aurait été menée par des gens travaillant pour le compte d'une agence gouvernementale, précise NBC.

Ce n'est pas la première fois que des « hackers russes » mythiques sont accusés d'attaques contre les sites de médias et d'institutions occidentales. Fin avril dernier, le porte-parole du Kremlin, Dmitri Peskov, commentait les rapports sur les attaques de « pirates informatiques russes » contre les réseaux informatiques américains et estimait qu'accuser Moscou de tous les maux « était devenu une sorte de sport ».

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.partiantioniste.com/actualites/le-pentagone-vise-par-une-cyber-attaque-russe-2492.html> :

---

# Le MIT réussit à imprimer un verre optiquement transparent | Le Net Expert Informatique

x	Le MIT réussit à imprimer un verre optiquement transparent
---	--

Lorsque l'on songe à l'impression 3D, bien souvent, la matière qui nous vient à l'esprit est le plastique fondu. Le Mediated Matter Group du MIT a opté pour une approche différente en utilisant un matériau transparent et apparenté au verre.

Logiquement baptisé G3DP (Ce n'est pas le nom d'un droïde de Star Wars, bien l'acronyme de Glass 3D Printing), il a été développé en collaboration avec le MIT's Glass Lab. L'idée est de passer par deux sas de température différente afin de façonner la matière, puis la refroidir sans l'abîmer ou la fragiliser.

Ainsi, la chambre supérieur chauffe la matière à 1 037.7 degrés Celsius et peut contenir suffisamment de matériau pour construire une seule composante architecturale. Celle-ci passe ensuite une seconde étape qui permet de la refroidir. L'imprimante 3D ne crée donc pas de verre à partir de zéro, elle retravaille plutôt la substance préexistante.

John Klein, Michael Stern, Markus Kayser, Chikara Inamura, Giorgia Franchin, Shreya Dave, James Weaver, Peter Houk et le Professeur Neri Oxman ont donc réussi à imprimer un verre optiquement transparent. Il est encore plus hypnotisant de s'extasier devant la vidéo.

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

---

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

Source :  
<http://fr.ubergizmo.com/2015/08/25/mit-imprimer-erre-optiquement-transparent.html>

---

# Votre crédit bientôt refusé à cause de vos amis Facebook ? | Le Net Expert Informatique



Votre crédit bientôt refusé à cause de vos amis Facebook ?

**Le réseau social a déposé un brevet qui permettrait aux banques de scruter les contacts d'un client afin de déduire sa capacité à rembourser un crédit.**

**Et si votre assureur savait tout de votre état de santé... Le smartphone tuera-t-il la carte bancaire (et les banques) ?**

A quoi joue Facebook ? Un brevet, déposé mardi 4 août, pourrait permettre aux banques d'examiner les relations d'un utilisateur sur le réseau social avant de lui accorder (ou non) un prêt.

Intitulé « Autorisation et authentification basée sur le réseau social de l'individu », le brevet entend proposer une nouvelle méthode d'authentification de l'internaute en fonction de ses amis Facebook, afin de limiter la propagation de spams (messages indésirables) et d'améliorer les résultats du moteur de recherche. Néanmoins, cette technique sera proposée à « des tiers », en particulier des banques. Le texte spécifie :

Lorsqu'un individu demande un prêt, le prêteur examine les scores de crédit des membres du réseau social de cet individu via un nœud autorisé. Si le score de crédit moyen de ces membres atteint le score de crédit minimum, le prêteur continue d'examiner la demande de prêt. Sinon, la demande est rejetée. »

En somme, si vos amis Facebook ont du mal à rembourser leurs prêts, alors la banque pourrait refuser de vous en accorder un. C'est une blague ? Non.

#### **Des start-ups américaines sur la brèche**

Généralement, les banques se basent sur l'historique financier pour déterminer la fiabilité d'un client, mais cette procédure est impossible si un tel historique n'existe pas. Du coup, les tentatives se multiplient pour éviter les personnes « à risque » en fonction des informations publiées sur les réseaux sociaux. Plusieurs start-ups s'en sont fait une spécialité.

Lenddo part du principe que si vos amis sont pauvres ou de mauvais payeurs, alors vous devez l'être aussi. L'entreprise américaine parcourt ainsi Facebook pour déterminer si le client potentiel est ami avec une personne ayant déjà remboursé un prêt en retard ou, pire, s'ils interagissent régulièrement.

La société LendUp, spécialisée dans le prêt en ligne, examine elle les comptes Facebook et Twitter des demandeurs, observant notamment le nombre d'amis et les interactions, afin d'accorder ou non le prêt.

De son côté, InVenture se base sur les données recueillies par le smartphone. Une application est proposée aux consommateurs pour gérer ses dépenses quotidiennes, tandis qu'un « score de crédit » est calculé en fonction des frais. Score qui sera fourni aux banques, afin de déterminer la capacité du client à rembourser un prêt.

Et même pas besoin d'appli : l'économiste Daniel Björkegren a montré qu'il suffit de croiser les dépenses des emprunteurs avec l'historique et la durée de leurs appels téléphoniques, pour réduire les défauts de paiement de 42%.



Illustration de l'ogre Facebook (Dimitris Kalogeropoulos/Flickr/CC)

#### **En France, l'étape du « partenariat »**

En France aussi, les rapprochements entre banques et réseaux sociaux commencent timidement. Début juillet, la Banque postale s'est associée avec Facebook pour que ses conseillers ouvrent des comptes sur le réseau social afin de rester en contact avec leurs clients. S'agira-t-il aussi de scruter les profils ? La banque ne s'épanche pas là-dessus, vantant la « prolongation de la relation client ».

A la mi-juillet, BNP-Paribas s'est alliée à Facebook, mais aussi Google, Twitter et LinkedIn afin d'améliorer « la pertinence de ses offres en fonction des attentes des clients ». La banque devrait ainsi bientôt proposer d'ouvrir un compte directement depuis Facebook.

La banque marche dans les pas du groupe BPCE (Banque populaire et Caisse d'épargne), allié à Facebook depuis la fin mai, dans une optique de proposer des « offres et produits innovants ». BNP-Paribas et BPCE n'ont en revanche pas précisé s'ils pourront récupérer des données de Facebook sur leurs clients.

CNN souligne néanmoins que les établissements bancaires rechignent encore à utiliser les données personnelles des réseaux sociaux pour évaluer le risque d'un crédit. « Ces données sociales n'indiquent pas nécessairement la fiabilité d'un client à rembourser un prêt à temps », note d'ailleurs John Ulzheimer, expert économique interrogé par la chaîne.

Alors, faut-il se précipiter sur son compte Facebook pour faire le tri parmi ses amis, avant que le nouveau brevet ne soit utilisé ? Pas sûr. Le site spécialisé Presse-citron tempère :

Les entreprises comme Google, Microsoft ou Facebook déposent de nombreux brevets, mais tous ne sont pas utilisés. Il est fort possible que Facebook n'utilise jamais ce brevet ou du moins pas la partie qui risque de vraiment fâcher ses utilisateurs. »

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://tempsreel.nouvelobs.com/tech/20150807.0B53843/votre-credit-bientot-refuse-a-cause-de-vos-amis-facebook.html#xtor=EPR-1-Actu8h-20150808>

Par Boris Manenti

---

# iPhone 6 à 1 euro – Une arnaque bien rodée | Le Net Expert Informatique



**iPhone 6 à 1 euro – Une arnaque bien rodée**

Diffusée partout, notamment sur les réseaux sociaux, cette arnaque qui débouche en fait sur des abonnements payants fait des dizaines de victimes, selon l'association de consommateurs.

Quand c'est trop beau, il faut se méfier... Allez dire ça aux victimes de Bernard Madhof qui promettait des placements assurant des rentabilité jamais vues ou à ceux qui ont cru à ces publicités proposant des iPhone 6 à 1 euro... Un iPhone à ce prix, personne ne devrait y croire, et pourtant...

Ils sont des dizaines à cliquer sur ces publicités qui pullulent actuellement sur la toile, notamment sur les sites de téléchargement ou via les réseaux sociaux. Au point que l'association de défense des consommateurs UFC Que Choisir s'en émeuve.

« Ces offres sentent le roussi à plein nez et pourtant, à en croire les messages qui arrivent sur différents forums Internet, leurs victimes se comptent par dizaines », souligne l'association qui a mené l'enquête.

Evidemment, en cliquant sur ces liens, point d'iPhone à l'horizon (ni de Galaxy S6 Edge, et encore moins d'Apple Watch) mais un abonnement surtaxé à un service quelconque.

#### Vrais-faux article de presse

« La page promotionnelle, au design et à la rhétorique soignés, invite l'internaute à saisir son adresse e-mail et à accepter les conditions générales. À l'étape suivante, il doit saisir ses coordonnées bancaires. Et, quelques jours plus tard, il constate qu'une somme rondelette, de 49 à 89 € selon les offres, a été débitée de son compte, en plus de l'euro prélevé initialement. Pire, ce prélèvement se répétera puisque l'internaute s'est en fait abonné à un site Internet de jeux en ligne, comme Rockyfroggy.com, un site de musique, comme Radioplanets.com, ou un club d'achat comme DealsOfToday.eu ou Wonkabonka.com », explique l'UFC.

Et ceux qui persistent à croire qu'ils recevront un jour leur précieux, peuvent attendre, longtemps. « En réalité, recevoir le produit promis n'est même pas garanti : il s'agit de lots que le nouvel inscrit peut potentiellement gagner, un gagnant étant le plus souvent « sélectionné » tous les 500 participants. L'euro payé par l'internaute lui ouvre en fait droit à une période d'essai de quelques jours aux services du site. Heureusement, d'après les témoignages lus sur les forums, ni la rétractation ni le désabonnement ne se semblent poser trop de problèmes ».

Le vrai problème, c'est la propagation massive et en augmentation de ces arnaques, sur Facebook, Twitter etc... « Il faut dire que Rockyfroggy, DealsOfToday et les autres usent de subterfuges variés et savent manifestement créer le « buzz ». Pour attirer les internautes à eux, ils arborent plusieurs « déguisements » dans lesquels ils glissent un lien vers leur page d'abonnement. Il peut s'agir d'une enquête de satisfaction émanant soi-disant de votre opérateur mobile, d'un jeu concours organisé par votre fournisseur d'accès à Internet, d'une note de blog imaginaire... »



Mieux, ces promos se glissent parfois dans des vrais-faux articles de presse. On a ainsi pu voir la charte graphique de La Tribune utilisée pour attirer le naïf... « Heureusement, les utilisateurs ne sont pas dupes », assure l'association, mais comme pour le spam, il suffit qu'un infime pourcentage clique pour faire le beurre de ces escrocs.

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.zdnet.fr/actualites/iphone-6-a-1-euro-l-arnaque-fonctionne-plutot-bien-alerte-l-ufc-39819222.htm>

# Les e-mails de hauts gradés de l'armée américaine piratés | Le Net Expert Informatique

 Economie - Les e-mails de hauts gradés de l'armée américaine piratés

**Le système de messagerie utilisé par 4 000 hauts gradés de l'armée américaine a été compromis fin juillet par des pirates informatiques et fermé par le Pentagone, selon les médias américains. L'enquête privilégie la piste russe.**

Comme un air de Guerre froide. Des « officiels » du Pentagone ont affirmé, jeudi 6 août, à la chaîne américaine NBC, que des pirates informatiques russes avaient réussi à s'introduire dans le système de messagerie informatique utilisé par 4 000 militaires et civils travaillant au Comité des chefs d'état-major interarmées.

La découverte de cette opération de cyberespionnage, lancée aux alentours du 27 juillet, a amené les autorités militaires à fermer entièrement le système de messagerie informatique utilisé par ces hauts gradés. Il ne sera remis à disposition du personnel qu'à la fin de l'enquête.

#### **Cyber Guerre froide ?**

Cette attaque est d'autant plus dommageable pour le Pentagone que ce n'est pas la première fois que des cyberespions s'engouffrent dans une faille du système de protection informatique des plus hautes sphères de l'État. Le président américain Barack Obama et le Département d'État (ministère américain des Affaires étrangères) ont ainsi déjà été pris cible ces quatre derniers mois.

Ces précédentes opérations avaient été attribuées par plusieurs entreprises de sécurité informatique à un même groupe : Cozy Bear. Leurs membres seraient russes, estime la société Kaspersky qui leur a consacré plusieurs rapports.

Interrogé par le quotidien britannique « The Guardian », Dmitri Alperovitch, le fondateur de la firme de sécurité informatique CrowdStrike, a noté une recrudescence des attaques informatiques russes visant des cibles américaines depuis l'instauration des sanctions économiques imposées depuis plus d'un an à la Russie par les États-Unis et ses alliés.

#### **Pas de vol d'informations classifiées**

Mais même si l'attaque contre le Pentagone est bien le fait de pirates russes, rien n'indique qu'ils ont agi sur ordre du Kremlin. Il peut s'agir de hackers « patriotes », souligne le site « Daily Beast », ou d'un groupe indépendant de pirates informatiques recruté par n'importe quel autre pays ou organisé pour espionner à sa place.

Ils ont à chaque fois utilisé la même technique : un e-mail piégé envoyé à des employés du service visé qui installe un virus dès que l'un d'eux clique sur un lien contenu dans le message. Des similitudes dans les messages et des traces laissées par les pirates sur les ordinateurs indiquent qu'ils ont utilisé les mêmes « armes » (comme un même type de virus personnalisé) pour commettre leur forfait.

Lors de l'attaque contre les hauts gradés du Pentagone, aucune information classifiée, qui ne s'échange que sur une messagerie spécifique, n'aurait été dérobée par ces pirates informatiques, ont affirmé ces sources à plusieurs médias américains. Reste que des échanges, comportant peut-être des informations personnelles sur les membres du premier cercle de l'armée américaine, ont été volés.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<http://www.france24.com/fr/20150807-emails-militaires-hauts-grades-armee-americaine-piratage-hacking-russie-pentagone>

Par Sébastien SEIBT

---

# La SNCB victime d'un piratage | Le Net Expert Informatique



La SNCB victime  
d'un piratage

## **Les systèmes de paiement électroniques de la société ferroviaire sont la cible d'une attaque informatique depuis plusieurs heures.**

Les systèmes de paiement électroniques de la SNCB sont la cible d'une attaque informatique depuis plusieurs heures. « Il s'agit d'une attaque d'origine externe dont les premiers signes ont été détectés mercredi soir, confirme la porte-parole, Nathalie Pierard. Nous travaillons avec les services de sécurité informatique du Fédéral pour protéger nos serveurs.» Ce sont les systèmes de paiement électroniques qui sont touchés, tant aux guichets qu'aux automates ou sur le mobile.

« Par période, les services sont fortement ralentis, poursuit Nathalie Pierard. À d'autres, ils sont inaccessibles. On a connu une accalmie vers midi puis les ralentissements ont repris en milieu d'après-midi. »

### **Pas de surfacturation à bord**

Suite à ce piratage dont l'origine est toujours indéterminée, la SNCB a décidé de ne pas faire payer la surfacturation de sept euros pour les billets achetés dans le train.

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.lesoir.be/956193/article/economie/2015-08-06/sncb-victime-d-un-piratage> :

# Un email constitue une commande ferme | Le Net Expert Informatique

 <p><b>Le Net Expert</b> <b>INFORMATIQUE</b> Protection des données personnelles Sécurité Informatique - Cybercriminalité</p>  <p><b>vous informe...</b></p>	<p><b>Un email constitue une commande ferme</b></p>
--	---

**Voici un arrêt qui pourrait bien, à nous Experts Informatique, nous servir de référence.**

**Denis JACOPINI**

Par un arrêt du 1er juillet 2015, la Cour de cassation considère qu'un courrier électronique envoyé par une société à un expert-comptable lui demandant une réponse étudiée sur trois questions précises, relatives à la fiscalité en Tunisie, constitue une commande ferme de prestation.

Une semaine après sa demande, l'expert-comptable lui avait envoyé sa consultation répondant aux questions posées ainsi que la facture correspondante.

La Cour casse le jugement du tribunal de commerce de Nanterre qui avait considéré qu'il s'agissait d'une simple prise de contact et d'une demande de renseignement général et des conditions financières d'intervention éventuelle.

Elle a estimé que l'email qui appelait à des réponses étudiées aux trois questions posées constituait une commande de consultation, présentée en termes clairs et précis.

Le lien vers la décision de la Cour de Cassation

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : [http://www.legalis.net/spip.php?page=breves-article&id\\_article=4690](http://www.legalis.net/spip.php?page=breves-article&id_article=4690)

---

# Fuite d'une ébauche du projet

# de loi numérique d'Axelle Lemaire | Le Net Expert Informatique

Fuite d'une ébauche du projet de loi  
numérique d'Axelle Lemaire

**Si la version « bêta » du projet de loi numérique n'a toujours pas été publiée (et ce alors qu'Axelle Lemaire avait indiqué que ce serait le cas « avant la fin du mois de juin »), Contexte vient de publier une version de travail du texte élaboré sous la houlette de Bercy. Ce document non définitif nous permet d'en savoir davantage sur la façon dont le gouvernement pourrait concrétiser ses ambitions.**

L'ébauche diffusée par nos confrères date de début juillet, avant que la piste d'une seconde loi relative au numérique – et portée cette fois par le ministre de l'Économie, Emmanuel Macron – ne soit confirmée par le gouvernement. « Selon nos informations, le texte a évolué depuis, et n'est toujours pas complètement stabilisé. Les réunions interministérielles de validation n'ont pas encore commencé » insiste d'ailleurs le journaliste Samuel Le Goff, pour bien faire comprendre que beaucoup de choses risquent de bouger d'ici à la publication de l'avant-projet de loi censé être soumis aux commentaires des internautes cet été.

Cette version de travail, longue d'une trentaine de pages, contient malgré tout plus de 80 articles. On y retrouve les principales mesures distillées au fil du temps par la secrétaire d'État au Numérique, Axelle Lemaire, ou même par Manuel Valls. Tour d'horizon.

#### Open Data

Ouverture par défaut des données publiques détenues par l'administration. L'État, les collectivités territoriales et les personnes chargées d'une mission de service public seraient tenus de diffuser automatiquement leurs documents administratifs communicables au sens de la loi CADA, dès lors que ceux-ci existent au format électronique. Aucune référence au format de mise en ligne de ces documents ne figure cependant dans cette version de travail. L'entrée en vigueur de ces dispositions est par ailleurs progressive : dans les six mois pour des « bases de données de référence définies par un arrêté du Premier ministre », puis deux ans pour les documents administratifs reçus ou produits après la promulgation de la loi, et enfin cinq ans pour l'ensemble des documents.

Principe de gratuité. La réutilisation d'informations publiques deviendrait gratuite, également par défaut. Des redevances pourront toujours être réclamées par des administrations, à condition toutefois que « le coût de la reproduction ou de la numérisation des documents administratifs concernés ou l'anonymisation des informations qu'ils contiennent représente une part significative de leurs ressources ». Un registre public serait spécialement créé afin de rassembler toutes les informations relatives à ces différentes redevances.

Création d'un « service public de la donnée ». Sous la houlette de l'Administrateur général des données, dont les missions sont gravées dans le marbre, ce service public de la donnée aurait pour objectif de faciliter la circulation de données entre administrations. Pour la première fois, il est prévu que des décrets puissent exiger « la transmission de données à l'administrateur général des données, lorsque cette transmission est nécessaire à la constitution ou à la mise à jour des données de référence ».

Statut pour les « données d'intérêt général ». Les délégués de services publics ou les organisations recevant des subventions de plus d'un million d'euros pourraient être contraintes de mettre en Open Data certaines données produites dans le cadre de leur mission, financée sur deniers publics. L'ouverture de données purement privées (environnement, énergie...) pourrait également être exigée par les pouvoirs publics, dès lors qu'il y aurait un « motif d'intérêt général, tenant notamment à leur contribution déterminante à la mise en œuvre d'une politique publique, à la recherche [publique] ou au développement d'activités économiques nouvelles ». Ces dispositions risquent toutefois d'évoluer suite aux travaux menés par la mission Cytermann (voir notre article).

#### Ouverture du code source des logiciels développés par l'État

Les « codes source des logiciels » figureraient expressément parmi la liste des informations publiques considérées communicables au sens de la loi CADA.

#### Protection des données personnelles

Plusieurs articles ont été rédigés afin que chaque utilisateur d'un service en ligne puisse obtenir la copie des données collectées à son égard, dans « un format électronique ouvert et permettant une réutilisation effective de ces données ». Des dispositions spécifiques aux emails ont également été insérées.

#### Renforcement des missions la CNIL

L'institution pourrait être « obligatoirement consultée sur tout projet de loi ou de décret comportant des dispositions relatives à la protection des données à caractère personnel ou au traitement de telles données ». Elle serait même autorisée à « prendre l'initiative de donner un avis » sur toute question relative la protection des données personnelles, notamment en direction du législateur.

#### Plus de pouvoirs pour la CNIL

Les sanctions prononcées par la Commission pourraient devenir bien plus dissuasives pour les géants du numérique : jusqu'à 3 millions d'euros ou, pour les entreprises, 5 % de leur « chiffre d'affaires annuel mondial ». On serait ainsi bien loin des 300 000 euros maximums prévus actuellement (et uniquement en cas de manquements répétés...). En cas d'urgence, la CNIL pourrait d'autre part ordonner au responsable d'un traitement de respecter la loi Informatique et Libertés dans un délai de 24 heures, contre 5 jours actuellement.

#### Action collective pour les litiges relatifs aux données personnelles

Sur le modèle des nouvelles actions de groupe, des internautes pourraient saisir les juridictions civiles par le biais notamment d'associations de consommateurs, et ce « afin d'obtenir la cessation d'une violation » à la loi Informatique et Libertés. Assez curieusement, ce dispositif ne fonctionnerait pas pour les traitements de données personnelles mis en œuvre dans le cadre d'un service public administratif.

#### Droit à l'oubli pour les mineurs

Le fait qu'une personne ait moins de 18 ans au moment où une donnée la concernant est collectée serait un « motif légitime » justifiant l'arrêt de son traitement, « sauf si la personne mineure était une personnalité publique ».

#### Droit de « mort numérique »

Chaque internaute pourrait laisser des directives concernant le devenir de ses données personnelles, en cas de décès. La personne désignée (ou, à défaut, les héritiers) auraient ensuite le pouvoir de se tourner vers les réseaux sociaux ou autres services en ligne pour obtenir par exemple la suppression des données ou du compte du défunt, etc.

#### Des pistes très variées

**Neutralité du Net.** Posant le principe que l'exploitant d'un réseau de communication électronique n'a « ni la connaissance ni le contrôle des informations reçues ou transmises par des tiers », des restrictions ne pourraient être mises en œuvre « que dans le respect des principes de non-discrimination, de proportionnalité, de nécessité et de transparence lorsque le niveau de qualité du service n'est pas garanti ».

**Définition positive du domaine public.** L'ébauche diffusée par Contexte comprend un article qui reconnaît expressément un « domaine public informationnel », composé premièrement des « informations, données, faits, idées, principes et découvertes, dès lors qu'ils ont fait l'objet d'une divulgation publique » ; deuxièmement des « objets qui ne sont pas couverts par les droits prévus dans le Code de la propriété intellectuelle ou dont la durée de protection légale a expiré » ; et troisièmement des « documents administratifs diffusés publiquement » par l'État, les collectivités territoriales, etc.

De nombreux autres sujets sont abordés, tels que la régulation des jeux d'argent en ligne, le renforcement des pouvoirs de l'ARCEP (le régulateur des télécoms), la loyauté des plateformes, etc. Sauf que certains de ces sujets auront plus vraisemblablement leur place dans l'éventuel projet de loi « Macron II », dont les mesures devraient être davantage tournées vers l'aspect économique. Résultat dans quelques jours, si le gouvernement se décide à publier (enfin) la version « bêta » du projet de loi numérique d'Axelle Lemaire.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.nextinpact.com/news/95876-fuite-d-une-ebauche-projet-loi-numerique-d-axelle-lemaire.htm>

Par Xavier Berne

---

# La Cnil met en demeure 13 sites de rencontre | Le Net Expert Informatique



La Cnil met en demeure 13 sites de rencontre

**Meetic, Attractive World ou Adopte un mec figurent dans une liste de 13 sites de rencontre mis en demeure par la Cnil pour leur mauvaise gestion des données de leurs membres.**

La Cnil veut éviter un scénario à la Ashley Madison en France. Ce site américain de rencontres extra-conjugales a été piraté la semaine dernière. Les données de quelque 37,5 millions de membres, aussi sensibles soient-elles, ont été dérobées. Alors la Commission nationale de l'informatique et des libertés a mené l'enquête auprès de plusieurs sites de rencontre... et annonce la mise en demeure de 13 d'entre eux.

Meetic, Attractive World, Adopte un mec, Easyflirt, Rencontre obèse, Destidyll, Forcegay, Mektoube, Jdream, Feujworld, Marmite love, Gauche rencontre, Celibest. C'est la liste retenue par la Commission, qui leur reproche à tous « de nombreux manquements à la loi informatique et libertés ».

Les voici :

- ne pas recueillir le consentement exprès des personnes pour la collecte de données sensibles, comme celles relatives à la vie et aux pratiques sexuelles, aux origines ethniques, aux convictions et pratiques religieuses ou aux opinions politiques ;
- ne pas supprimer des données de membres ayant pourtant demandé leur désinscription ou ayant cessé d'utiliser leurs comptes depuis une longue durée ;
- mettre en œuvre des fichiers afin d'exclure des personnes de l'accès au service sans avoir procédé à des demandes d'autorisation auprès de la Cnil ;
- ne pas informer correctement les internautes de leurs droits (accès, suppression, rectification) ni des conditions dans lesquelles des cookies sont déposés sur leur ordinateur.

Dépourvue de pouvoir de sanction, la Cnil peut désigner un rapporteur qui décidera, lui, d'une peine –



Crédit : Pic Rider (Fotolia)

### **Le spectre d'une mauvaise pub**

Concrètement, ce sont les sociétés éditrices (8 au total) des sites de rencontre qui sont mises en demeure. Habituellement, une telle procédure n'est pas rendue publique par la Cnil. Une exception que justifie la Commission par la « sensibilité des données en cause » ainsi que « le nombre de personnes concernées ».

Les entreprises visées ont un délai de trois mois pour se conformer à la loi. « La clôture de chacune des procédures fera également l'objet d'une publicité », agite la Cnil, pour les motiver à améliorer leur politique de gestion des données. Dans le cas contraire, elle désignera un rapporteur chargé d'étudier des sanctions pouvant atteindre 300 000 euros selon Les Echos. Mais surtout, une mauvaise publicité leur sera faite.

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://pro.clubic.com/legislation-loi-internet/cnil/actualite-775064-cnil-sites-rencontre.html>

Par Thomas Pontiroli

---

# Les objets connectés deviendraient des témoins ? | Le Net Expert Informatique



Les objets connectés deviendraient des témoins ?

Aux Etats-Unis, on commence à produire les données de bracelets connectés pour démentir ou renforcer un témoignage. Ces données pourraient aussi entrer dans nos tribunaux, ce qui n'est pas sans poser question.

À quel service les objets connectés « portables », ces bracelets ou ces montres qui permettent de mesurer votre activité physique, vos dépenses en calories et même parfois votre humeur ? À mieux se connaître, répondent les auteurs. A mesurer une vie plus saine. Mais une histoire récente, aux Etats-Unis, montre que ces objets peuvent aussi servir lors de votre procès.

#### Et là, son FBIbit a lâché la merve

Une femme de 43 ans qui avait porté plainte pour viol a été démentie par les données de son FBIbit (bracelet connecté mesurant l'activité et le sommeil). L'histoire a été rapportée la semaine dernière par la chaîne d'information locale ABC 27 News. La femme avait affirmé aux enquêteurs qu'un homme s'était introduit au milieu de la nuit dans sa chambre et l'avait emmenée avec un couteau pointé de la crosse. Mais son objet a contredit ses dires : « Elle avait affirmé qu'elle avait perdu sa montre de fitness en résistant à son agresseur, mais l'objet a été retrouvé intact dans le couloir, près de la salle de bain (où elle avait dit que s'était déroulé le viol, ndr) ». Selon le chef d'enquêteur, quand les enquêteurs ont téléchargé son activité de fitness, ils se sont aperçus que la femme n'avait pas dormi cette nuit là et qu'elle avait marché tout le temps, au lieu de dormir comme elle l'avait affirmé. Et plus de ces données, les enquêteurs n'ont trouvé aucune trace de pas dans la neige autour de la maison (les faits se sont déroulés en hiver) ni aucune trace d'intrusion. En conséquence, la femme a été incriminée pour fausse déclaration et altération de preuves.

#### Des grosses balances... ou Google Glass

Mélanie, en novembre 2013, à Calgary (Canada), une femme, qui demandait à être indemnisée pour préjudice corporel après un accident, a utilisé les données de son bracelet connecté pour prouver que son activité physique était réduite depuis son accident. (Une histoire alors analysée par Olivier Extrachiste.) Les objets connectés arrivent donc dans les tribunaux. Et selon les avocats cités dans la presse américaine (ici ou ici, par exemple), cette tendance est appelée à grandir. Dans Wired, un avocat américain se demandait ainsi : « [Les données des objets connectés] pourraient-elles être utilisées comme alibi ? » Ou encore : « Est-ce qu'on pourrait utiliser les données d'un FBIbit pour prouver qu'un cardiologue avait fait preuve de négligence, en ne retraçant pas l'exercice d'un patient ? » Ces objets peuvent donner des indications sur les activités de celui ou celle qui le porte, mais aussi sur la façon dont il ou elle se trouve, grâce à des fonctions de personnalisation. Les plus sophistiqués, comme les Google Glass, font aussi des photos ou des vidéos, ainsi que des recherches sur le Web. On voit bien l'usage que policiers, assureurs ou autres pourraient faire de ces données, en les restaurant contre son propriétaire.

#### Démenti dans vos préférences

De France, le cas ne s'est encore jamais présenté, mais, explique Me Clarisse La Corre, avocate au cabinet Wigo, il est tout à fait envisageable : « Selon la loi, les infractions peuvent être établies par tout moyen de preuve et c'est le juge qui décide ensuite selon son intime conviction ». À cheval entre données personnelles et données médicales, ces informations sont souvent appelées « données de biométrie ». Elles sont protégées par la loi « Informatique et liberté », mais dans le cas d'un procès, cette protection peut être levée par l'instruction. Parce qu'elles sont également recevables et qu'elles sont ensuite soumises au contradictoire, c'est-à-dire être débattues par les deux parties, les données des objets connectés peuvent tout à fait être présentées devant un tribunal.

#### Leurs données sont-elles fiables ?

Pourtant, ces données sont loin d'être totalement fiables. Les objets connectés buguent. Comme l'a récemment montré notre collègue Thomas Schepers, les appareils connectés peuvent buguer et les données récoltées ne reflètent pas forcément vos activités.

#### Ils sont faciles à duper.

Pas besoin de réfléchir longtemps pour voir comment on pourrait duper le bracelet connecté : il suffit de le faire porter par un complice ou de l'apposer à un animal domestique ou comportement pas trop erratique. Ou encore de rester assis à son bureau en bougeant ! Les pieds très vite pour faire croire qu'on fait un jogging.

#### Ils « mesurent » selon des critères qui changent de machine en machine et sont déterminés par des algorithmes inaccessibles.

Comme le rappelle la chercheuse américaine Kate Crawford dans The Atlantic, les mesures qu'effectuent ces outils dépendent de la façon dont ils ont été programmés et sont souvent opaques.

#### Le Jadeone UP, Nike Fuelband, Fitbit et Mitting's Pulvie (différents modèles de bracelets connectés, ndr) ont chacun des modes de fonctionnement particulier : certains comptabilisent les mouvements de bras comme de la marche (merveilleux, si vous voulez comptabiliser l'écriture comme de l'exercice), d'autres comptabilisent difficilement le vélo comme une activité physique.

La fonction de mesure du sommeil emploie des méthodes assez grossières pour faire la différence entre sommeil léger et sommeil profond. [...] »

Un bracelet Jadeone Up (Ashley Baxter/Flickr/CC)

#### La chercheuse ajoute, faisant référence à l'exploitation de ces données :

« Ces données sont rendues encore plus abstraites par des entreprises d'analytique qui créent des algorithmes propriétaires, pour les comparer à leur standard de ce qu'est une personne normale "en bonne santé" ».

#### Effectivement, explique Me La Corre, à mesure que l'on s'interroge sur le statut de ces objets, on découvre leurs limites :

« La question de la fiabilité des données de ces objets va se poser de façon aiguë. Pour l'instant, nous manquons de recul sur ces choses-là parce qu'elles sont très récentes. D'où l'intérêt de la soumettre à la discussion des deux parties, qui sert de garde-fou. »

#### Les données par elles-mêmes ne signifient rien : elles s'intègrent dans un faisceau de preuves, et doivent toujours être contextualisées.

#### Au-dessus des témoins humains.

On suspecte les données de biométrie utilisées contre leur propriétaire, on comprend aussi même ce que sont vraiment les objets connectés. Ainsi, réfléchissant sur ce thème, la chercheuse Kate Crawford, qui travaille sur les implications du big data et des objets connectés, rappelle l'ambiguïté fondamentale des objets connectés : « Ils se présentent comme les instruments d'une meilleure connaissance de soi. Mais sont aussi des « informateurs » qui collectent des données et les transmettent au fabricant et à des tiers – potentiellement à des assureurs et des employeurs. Plus profondément, c'est le statut que l'on veut donner à ces données qui est en jeu. Kate Crawford met en garde contre la tentation d'une « vérité fondée sur les données », où celles-ci finiraient par sembler plus fiables – parce que plus neutres – que l'expérience des témoins. »

#### Donner le prioritarité aux données, qui sont irrégulières et peu fiables, sur les témoignages humains, cela signifie que l'on donne la priorité à l'algorithme. Or ces systèmes sont imparfaits – comme peut l'être le jugement humain. »

Les données des objets connectés ne sont que ça, des données : des mesures qu'il faut contextualiser et comprendre, et surtout ne pas prendre pour argent comptant.

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybersécurité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

#### Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPIN

Tel. : 06 39 73 39 32

Formateur n°93 84 82041 94

Expert informatique assésuré et formateur spécialisé en sécurité informatique, en cybersécurité et en déclaration à la CNIL. Denis JACOPIN et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Est-ce-à vous plaît ? Page 1

De avis ? Laissez-nous un commentaire !

Source : <http://me93.nouvelobs.com/2013/07/01/quand-les-objets-connectes-temoignent-a-proces-contre-26000>