TVA. Bercy s’attaque aux systèmes informatiques des fraudeurs | Le Net Expert Informatique

	TVA. Bercy s’attaque aux systèmes informatiques des fraudeurs

Depuis ces derniers jours, le ministère de Finances a mené diverses opérations qui visent les systèmes informatiques des entreprises fraudeuses à la TVA.

Une opération ayant mobilisé « une centaine d'agents » de divers services rattachés à Bercy, en liaison avec le ministère de l'Intérieur, a selon un communiqué permis de démanteler « une filière de diffusion d'un programme informatique spécifique dans le secteur pharmaceutique », en procédant à des perquisitions à la fois des locaux de l'éditeur de ce programme informatique, mais aussi de « certains de ses revendeurs et clients utilisateurs ».

Des « conséquences fiscales et juridiques »

Peu avant, la Direction générale des finances publiques (DGFip) avait, toujours selon le communiqué, mené une « opération d'envergure auprès de 200 utilisateurs » d'autres programmes informatiques frauduleux, cette fois dans le commerce de détail.

Il s'agit selon le ministère de la première mise en œuvre de « la nouvelle procédure de contrôle inopiné informatique ». Ces opérations auront des « conséquences fiscales et juridiques », avertit enfin Bercy.

140 milliards d'euros de recette annuelle

La fraude à la TVA, parfois très sophistiquée, coûte cher à l'État français, même si le phénomène est difficile à mesurer.

En 2013, la Commission européenne avait estimé le manque à gagner pour la France à une trentaine de milliards d'euros par an, tandis que le ministère des Finances avait plutôt évoqué un ordre de grandeur de 10 milliards. La taxe sur la valeur ajoutée représente à elle seule la moitié des recettes fiscales de l'État, auquel elle rapporte près de 140 milliards d'euros chaque année.

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

Source : http://www.ouest-france.fr/tva-bercy-sattaque-aux-systemes-informatiques-des-fraudeurs-3378229

Les 5 dangers du projet de loi sur le renseignement | Denis JACOPINI

	**Les 5 dangers du projet de loi sur le renseignement**

Dernière ligne droite pour le projet de loi sur le renseignement. Le vote solennel du texte est prévu ce mardi 5 mai à l'Assemblée, malgré une mobilisation des opposants, lundi soir au Trocadéro, à Paris.
Que dit le texte ? Au fil des débats, les députés ont fait évoluer le projet de loi. « Il a été considérablement enrichi », estime son rapporteur, Jean-Jacques Urvoas (PS), dans une note envoyée aux députés dont « l'Obs » a eu connaissance. Au total, 260 amendements ont été adoptés. Cela répond en partie aux demandes des adversaires du texte, mais ne lève pas toutes les inquiétudes, loin de là.

Ce que l'Assemblée a modifié :
Une commission de contrôle renforcée
Est surtout renforcé « la composition, l'indépendance et les pouvoirs de la [nouvelle] Commission nationale de contrôle des techniques de renseignements » (CNCTR). Celle-ci remplacera l'actuelle Commission nationale des interceptions de sécurité (CNCIS) et, comme réclamé dans « l'Obs » par son actuel président, cette nouvelle instance disposera d'un « accès aux locaux des services, aux dispositifs de traçabilité, aux opérations de transcription, d'une saisine élargie du Conseil d'Etat ». De plus, les renseignements collectés seront bien centralisés par le Groupement interministériel de contrôle (GIC), que « l'Obs » a pu visiter en exclusivité.

Des professions moins exposées
Le texte exclut désormais certaines professions de la procédure d'urgence. Pour les magistrats, les avocats, les journalistes et les parlementaires, les écoutes ne peuvent être mises en œuvre que sur autorisation du Premier ministre, après avis de la commission. (Art. L. 821-7)

Un statut de lanceur d'alerte
De même, un « statut de lanceur d'alerte a été créé afin d'apporter une protection juridique à tout agent souhaitant révéler des illégalités commises ». N'est en revanche pas précisé si ce statut pourra être étendu à tous ceux qui révèlent des illégalités, à la manière d'Edward Snowden sur la NSA.

Les hackers plus fortement sanctionnés
Les députés ont également profité du texte pour renforcer l'arsenal de sanctions contre les hackers. Dans le sillon de la cyberattaque contre TV5 Monde, ils ont décidé de doubler les sanctions pécuniaires pour tout piratage (actuellement puni au maximum de 75.000 euros), voire de les tripler s'il s'agit d'un service de l'Etat.

Un fichier des personnes mises en cause pour terrorisme
Le gouvernement a également profité de cette loi pour créer un nouveau fichier (FIJAIT) qui recensera les noms et adresses de toutes les personnes condamnées ou mises en examen pour terrorisme.

Malgré des améliorations notables du texte, certains points continuent de poser problème.

1 – Le Premier ministre, seul maître à bord
La loi dote les six services de renseignement français de nombreux moyens supplémentaires pour enquêter, et la plupart n'auront plus besoin de l'aval d'un juge. En effet, le Premier ministre se positionne comme seul décisionnaire.
Les autorisations sont délivrées, après avis de la CNCTR, par le Premier ministre », pointe le texte.
Surtout que le Premier ministre pourra passer outre l'avis de la CNCTR, mais devra alors motiver sa décision (et risquer une saisine du Conseil d'Etat). Et tout ceci s'applique, sauf « en cas d'urgence absolue »…

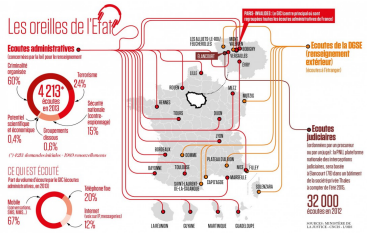
2 – Des données conservées longtemps
Afin de surveiller une personne, le projet de loi prévoit de nombreuses interceptions à distance (e-mails, conversations téléphoniques, SMS…) mais aussi la pose de micros et caméras dans des lieux ou des véhicules. Le texte prévoit que l'ensemble des renseignements ainsi collectés seront détruits au terme de certaines durées :
• 30 jours pour les correspondances,
• 90 jours pour les sonorisations, les géolocalisations et les images vidéo,
• 5 ans pour les données de connexion, aussi appelées métadonnées (qui donnent le détail de qui écrit un e-mail à qui, à quelle heure, etc.).
Et, en cas de cryptage des données, ces délais ne s'appliquent qu' »à compter de leur déchiffrement ».

3 – Eviter de croiser la route d'un suspect
Le projet de loi prévoit que les mesures de surveillance seront utilisées à la fois pour les suspects, mais aussi pour les « personnes appartenant à [son] entourage » s'il « existe des raisons sérieuses de croire [qu'elles ont] joué un rôle d'intermédiaire, volontaire ou non ». En somme, n'importe qui se trouvant au mauvais endroit, au mauvais moment, et ayant croisé une mauvaise route, pourra être mis sous surveillance.

Lors de la manifestation contre le projet de loi sur le renseignement, le 13 avril (CITIZENSIDE/ANTHONY DEPERRAZ/AFP)

4 – Tous suspects sur internet
Le projet de loi entend mettre à profit les opérateurs internet. Fournisseurs d'accès, moteurs de recherche, réseaux sociaux… Tous pourront fournir « en temps réel » les données techniques de connexion des internautes suspectés de terrorisme. Concrètement, il s'agit de pister une connexion (exprimée par une adresse IP) pour savoir quel site elle a visité, à quelle heure, si elle a envoyé un message Facebook à telle personne, si elle a tapé tel mot clef sur Google…
Le texte souhaite aussi contraindre les opérateurs internet à « mettre en œuvre sur leurs réseaux un dispositif destiné à détecter une menace terroriste sur la base de traitements automatisés ». Concrètement, les services de renseignement installeront une « boîte noire » dotée d'un algorithme qui passera au crible l'ensemble du trafic internet pour détecter automatiquement des internautes soupçonnés d'être des terroristes. A terme, cette boîte noire pourra être mise en place chez les fournisseurs d'accès à internet, mais aussi les Américains Google, Facebook, Apple ou Twitter.
L'ensemble du système surveille l'ensemble des internautes de manière anonyme pour détecter des « signaux faibles ». Et, en cas de suspicion, les opérateurs devront dénoncer la personne correspondant aux enquêteurs.
La CNCTR aura accès « au code source » de cette boîte noire afin de limiter la collecte des données aux seuls terroristes. Du moins, tant qu'un décret n'a pas étendu le champ d'action de ce dispositif qui s'apparente à « une surveillance de masse » inspirée par l'agence de renseignement américaine NSA.

5 – Surveiller les terroristes, mais pas seulement
Finalement, il convient de rappeler que, malgré les présentations du texte par François Hollande ou Manuel Valls, il ne s'agit pas d'une loi anti-terroriste, mais bien d'un texte sur le renseignement. Le projet prévoit sept finalités pour recourir aux diverses techniques de renseignement :
• l'indépendance nationale, l'intégrité du territoire et la défense nationale,
• les intérêts majeurs de la politique étrangère et la prévention de toute forme d'ingérence étrangère,
• les intérêts économiques, industriels et scientifiques majeurs de la France,
• la prévention du terrorisme,
• la prévention des atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la sécurité nationale ou de la reconstitution de groupements dissous,
• la prévention de la criminalité et de la délinquance organisées,
• la prévention de la prolifération des armes de destructions massives.
Pour rappel, en 2014, 60% des écoutes administratives visaient la criminalité organisée, 24% le terrorisme, 15% la sécurité nationale (contre-espionnage), 0,6% les groupements dissous, et 0,4% la protection du potentiel scientifique et économique. Depuis l'attaque meurtrière contre « Charlie Hebdo », la part dédiée au terrorisme est montée à 48%.



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

Note de Jean-Jacques Urvoas publié par NouvelObs.com

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

Source : http://tempsreel.nouvelobs.com/loi-renseignement/20150504.OBS8368/les-5-dangers-du-projet-de-loi-renseignement.html?cm_mmc=EMV-_-NO-_-20150505_NLNOACTU08H-_-les-5-dangers-du-projet-de-loi-renseignement##xtor=EPR-1-Actu8h-20150505
Par Boris Manenti

Loi sur le renseignement ou pratique de la surveillance automatisée ? | Le Net Expert Informatique

Un expert du Big Data m'a adressé ce texte. Il y expose clairement pourquoi, selon lui, la « détection automatisée de comportements suspects » prévue par la Loi Renseignement est très dangereuse. En un mot, mettre les gens dans des cases au moyen d'un algorithme forcément imparfait, ce n'est pas grave s'il ne s'agit que d'envoyer de la publicité ciblée, mais ça l'est beaucoup plus s'il s'agit d'envoyer des policiers interpeller des gens chez eux à 6 heures du matin.

Je vous livre ce texte :
« Depuis plusieurs années je travaille sur le big data appliqué au marketing en ligne. J'ai les mains dans le moteur du matin au soir, et lorsque j'ai appris quelle était la teneur du projet de loi qui devrait être voté le 5 mai prochain, je n'ai pu m'empêcher de frémir en essayant d'imaginer les usages possibles des techniques et des procédés annoncés. Voici quelques réflexions qui me sont venues sur ce dispositif qui pourrait transformer radicalement notre société. Je ne suis pas certain que nos députés aient une idée claire de la boîte de Pandore qu'ils s'apprêtent à ouvrir sur ordre de l'exécutif.
Je me souviens de l'aventure advenue il y a longtemps à l'un de mes oncles, militant fortement engagé dans une association (pacifique) classée franchement à gauche. Il avait vu un jour débarquer chez lui deux personnes des Renseignements Généraux, munies d'un gros dossier qui recensait en détail toutes ses activités. Juste histoire de lui faire comprendre qu'ils savaient qui il était, où il habitait, ce qu'il faisait – pourtant rien d'illégal – et qu'on le tenait à l'oeil. Une simple visite de courtoisie; ou peut-être peut-on appeler ça de l'intimidation? Tout ça s'est passé bien avant la généralisation d'Internet, des fichiers numériques et des téléphones portables. Aujourd'hui, le dossier n'aurait peut-être pas pu être porté sous le bras, ou plutôt si, sur une clé USB, contenant dix ou dix mille fois plus d'informations.
Je me souviens aussi, lorsque j'ai commencé à travailler sur des clusters, du choc que j'ai ressenti la première fois où nous avons tracé une carte utilisant des adresses IP de visiteurs (il est très facile d'obtenir des données géographiques assez fiables pour une adresse IP résidentielle). La carte mettait en évidence de manière saisissante des comportements liés directement à la provenance géographique. Les gens de mon quartier (on était déjà descendus à une échelle plus fine que celle d'une ville) avaient exactement les mêmes comportements que moi; je me suis vu dans la carte. Mon estime en a pris un coup, car j'étais rétrogradé en une seconde au rang de mouton.Mais j'ai réalisé, en regardant ce découpage coloré, à quel point ce nouvel outil nous offrait une puissance et une justesse d'analyse dont nous n'avions même pas rêvé.
Parmi les nombreux problèmes que posent cette loi, se trouve la pose de « boîtes noires » chez les fournisseurs d'accès et les hébergeurs, espionnant potentiellement tout le trafic Internet. Un malentendu assez fréquent est que l'on saura ce que vous faites en inspectant effectivement vos différentes activités en ligne. Qu'on cherchera *individuellement* vos traces d'activité suspecte. Et qu'il vous suffira de visiter quelques sites pour être visé par des investigations plus poussées. Et l'on se dit que l'on n'a rien à craindre, puisqu'on n'a certainement rien de commun avec les terroristes en puissance. Mais ce n'est pas comme ça que ces systèmes fonctionnent.
Pour qu'ils soient efficaces, ils ont besoin de modèles, dont l'utilisation s'apparente à des techniques de pêche au chalut. On attrape tout, on trie, et on garde ce qui est intéressant. Mais comment savoir ce qui est intéressant a priori ? Justement, on ne peut pas vraiment. Ça fonctionne en gros comme ça :

• Première phase, on collecte tout en vrac, sur beaucoup de monde, pendant un moment.
• Deuxième phase, on identifie le groupe d'individus que l'on recherche (mais pas directement, ou en tout cas pas uniquement en utilisant ces données), et on l'indique au système.
• Troisième phase, à partir des données qui ont été collectées sur les membres identifiés de ce groupe, le système fabrique un modèle, selon différentes méthodes.
• Et quatrième phase, on identifie tous les autres, éventuellement vous, qui ne font pas partie du groupe, parce qu'ils se conforment au même modèle.
• On continue à alimenter le système itérativement, on affine le modèle, et on continue.

Dans la pratique, le jugement humain intervient, mais si l'on cherche à étendre ce système, on peut laisser aux machines le soin d'en faire plus, et finalement opérer elles-mêmes le choix des marqueurs d'une activité « suspecte ». C'est à la fois un peu moins inquiétant (vous pouvez continuer sereinement vos recherches de nitrate d'ammonium en ligne si vous êtes agriculteur sans être soupçonné de vouloir fabriquer une bombe) et pire, car à mesure que la quantité de données disparate augmente, il va devenir compliqué de savoir pourquoi une personne a un score élevé dans une catégorie recherchée. Il ne s'agit pas de cases virtuelles que le système coche au fur et à mesure, mais de relations mathématiques et d'enchaînements entre des données dont le sens est éventuellement complètement obscur. Et on peut fort bien tomber dans la mauvaise case.

Dans le domaine du marketing, tomber dans la mauvaise case n'est pas dramatique : une publicité mal ciblée ou les recommandations absurdes d'un site de commerce en ligne n'ont jamais changé dramatiquement la vie de quiconque ; j'avais eu un bel exemple de ce genre sur le plus gros site d'e-commerce du monde il y a quelques années, où mes collègues et moi-même n'avions vu l'espace d'une matinée que des recommandations étonnantes, composées à 50% environ de prothèses de jambes. Bug manifeste du moteur de recommandations, dont nous avions eu toutes les peines du monde à nous extraire. Une fois que vous êtes lancé dans un tunnel, dans ce domaine, il est parfois difficile d'en sortir. Donc cette fois-là c'était plutôt amusant. Si un problème semblable advient sur des systèmes de surveillance, la personne qui atterrira d'un coup sur les radars des services de renseignement risque de trouver l'expérience moins ludique.

Mais on ne pourra pas surveiller tout le monde, se dit-on. En fait, si, on peut. Une des caractéristiques des systèmes dédiés au big data c'est la scalabilité linéaire. En termes moins techniques, ça signifie que pour doubler votre capacité de stockage ou de traitement, il suffit grosso modo de doubler le nombre machines dans le cluster. Un cluster, c'est un ensemble de machines (des centaines, des milliers ou plus) qui fonctionnent en parallèle et stockent chacune une partie des données dont vous les nourrissez en permanence. Le principe est d'assembler toutes ces données en les découpant d'abord en de multiples morceaux, traités en parallèle, chacun sur une machine. Au lieu d'un seul programme, vous avez mille programmes qui traitent chacun un morceau de données, tournant sur mille machines, comme s'il s'agissait d'un seul ordinateur gigantesque. Vous avez deux fois plus de données à stocker ? Rajoutez autant de machines et des disques durs. Vos traitements prennent trop de temps ? Rajoutez des machines. La beauté de la chose, c'est que ces systèmes ne sont pas plus durs à gérer quand vous passez de cent à dix mille machines. La même équipe peut s'en charger, la seule limite est le budget. Le système est extensible à l'infini. La capacité et le prix des disques durs aujourd'hui rendent éventuellement inutile la purge des données; on peut tout conserver à tout jamais. Ce n'est qu'une question de moyens.

Alors bien sûr, il faut des analystes (des statisticiens ou des spécialistes de l'intelligence artificielle) et des programmeurs pour créer les programmes qui vont établir des relations entre des données disparates. Mais là encore, beaucoup de choses peuvent être accomplies par des équipes réduites. Les algorithmes qui permettent de partir à la pêche dans l'océan des données sont maintenant rôdés, et il n'est point besoin de réinventer la roue à chaque nouveau problème. L'important est de poser la bonne question, le reste n'est qu'un détail d'exécution. De plus, grâce la puissance de ces architectures, on peut poser de multiples questions dans un temps raisonnable, ce qui n'a jamais été possible auparavant. On peut affiner la question posée, jusqu'à un grand niveau de détail. On peut obtenir des réponses à des questions que l'on n'a pas pensé à poser. Et plus le volume de données est important, plus la fiabilité des réponses, en général, augmente. Enfin, ces données restent accessibles sans délai et s'offrent pour toujours à de nouvelles analyses. Elles permettent de définir des modèles de plus en plus fins, auxquels sont comparées en temps réel les nouvelles données qu'ingurgite en continu le système. Elles permettent de classer, d'identifier, et souvent de prévoir.

Cela dit, et c'est là que la prétention d'empêcher les actes terroristes trouve sa limite, elles permettent de prévoir en termes de probabilités. Elles permettent de vous classer dans un groupe, pas de savoir vraiment si oui ou non vous allez effectivement faire telle ou telle chose, ni quand. A moins que vous n'ayez acheté une grande quantité du nitrate d'ammonium suscité par CB (ce qui serait franchement stupide), que vous ne fréquentiez assidument des individus connus pour leurs appels à la guerre sainte, et que vous n'ayez donné rendez-vous à vos copains par e-mail pour le feu d'artifice, le système ne va pas pouvoir dire quel jour et à quel endroit vous allez poser une bombe artisanale. A moins de disposer des données de centaines de personnes effectivement parties faire le jihad, et qu'elles ne permettent de construire un modèle fiable, ce qui reste à démontrer, il ne pourra pas non plus identifier de manière fiable le départ des prochains candidats. On baigne là dans l'illusion technologique. Ainsi, malgré les considérables moyens déployés aux Etats-Unis, il ne semble pas que la NSA ait atteint dans ce domaine des records d'efficacité. La France ferait-elle mieux ?

Donc, à quoi ça sert ? N'étant pas dans le secret des décideurs, je ne peux qu'imaginer : si j'étais au pouvoir et que j'avais ce gros jouet à disposition, je pourrais toujours avoir une longueur d'avance sur… tout ! Pour prévoir les grèves, les mouvements sociaux, l'agitation étudiante, les ZAD, les contestations diverses, les tendances pour les élections. Même pour la politique étrangère, l'intelligence économique, les possibilités sont infinies. Un outil extraordinaire, mille fois meilleur et plus riche en volume que tous les sondages et les compte-rendu des ex-RG. Les utilisateurs de big data dans le domaine du marketing le savent très bien: les gens mentent (sans le savoir, et croient donner des réponses sincères), mais leurs actions, elles, ne mentent pas.

Exemple au hasard, les « intérêts économiques essentiels de la nation » (un parmi la liste très large des objectifs de la loi). J'imagine fort bien des IMSI-catchers dans le quartier de la Défense, à l'écoute des managers discutant de contrats avec des firmes étrangères concurrentes de firmes françaises. Étant donnée la perméabilité entre les grandes entreprises et la haute fonction publique, je peine à croire qu'aucun conseil amical ne filtrera jamais des services de renseignement vers les directions de ces entreprises. Bien sûr on n'écoutera pas toutes les conversations des concurrents – ce qui demande trop de temps – mais il est déjà démontré qu'il suffit de connaître la liste de vos correspondants, la durée et la fréquence de vos appels pour savoir à peu près tout de votre activité et de vos projets. Les fameuses métadonnées, dont les partisans de la loi vantent la quasi-innocuité, suffiront pour tout leur dire sur vous. Le secret des affaires ? Obsolète. On pourrait faire un concours de pronostics sur tous les usages possibles de cette loi, vu son champ d'application tellement large. On serait sans doute encore à cent lieues de prévoir ce qui se passera exactement.

Mais il y a le contrôle par la commission, objectera-t-on. Je l'imagine cette commission, inondée de requêtes, combien par jour ? Dix, cent, mille ? Combien de temps passé sur chacune d'entre elles ? Comment prétendre qu'il s'agira d'autre chose qu'une chambre d'enregistrement ? Les moyens techniques permettront de rédiger des demandes par centaines, sans effort, à tel point que le contrôle de celles-ci ne deviendra plus qu'un processus de pure forme, sous l'avalanche continuelle. De toutes manières, qui garantira l'indépendance et la compétence des nominés ? Comment prétendre que remplacer tous les juges par une seule commission n'effectuant qu'un contrôle a posteriori, et dont le silence vaut accord, pourra garantir les droits de chacun ? Comment croire qu'un seul « expert technique » pourra valider tous les algorithmes utilisés ? Rien que ce dernier point me semble absurde. Ensuite, il y a la durée de conservation des données, qui est limitée. Techniquement, purger des données disparates est déjà un peu compliqué. Quant à purger des données dérivées des données brutes, pour de multiples raisons, c'est encore plus complexe. Il faudra que cet impératif soit au coeur du système dès le départ pour que cela ait une toute petite chance de fonctionner. Les paris sont ouverts.

L'exécutif se retrouverait donc doté d'un outil par définition opaque, surpuissant, qui lui permettrait de s'abstraire presque totalement du pouvoir judiciaire. Exécutif élu, rappelons-le, pour cinq ans. C'est très court, et c'est prendre un bien gros pari sur l'avenir que de mettre dans les mains de quelques personnages-clés une arme qui permet de contrôler aussi totalement tous les aspects de la vie des personnes. Et de les influencer, voire de les contraindre, quelle qu'en soit la raison. Mais après tout, si vous n'avez ni l'intention de vous syndiquer, ni de donner un avis controversé sur un forum, ni de tromper votre conjoint(e), ni de revendiquer quoi que ce soit, ni de critiquer qui que ce soit, en somme de ne pas faire quoi que ce soit que vous ne vouliez pas que la terre entière apprenne, qu'avez-vous à craindre ? C'est ce qu'on appelle une société de surveillance. La vie privée est un concept désormais obsolète, c'est presque inévitable. »

Voilà, maintenant que vous avez lu ce texte qui est bien plus argumenté que l'exemple caricatural que je vous avais donné, je vous invite à vous faire votre propre opinion, et à le partager autour de vous si vous jugez que cela peut être utile. N'hésitez pas à le transmettre aux députés qui, demain, voteront sur ce projet de loi !

PS : si mon ami a choisi l'anonymat, ce n'est pas par crainte de la police ou de la justice de la République, mais juste parce qu'il ne souhaite pas qu'un lien soit fait avec son employeur.

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

Source : http://www.zdnet.fr/actualites/loi-renseignement-un-ami-expert-du-big-data-explique-le-danger-de-la-surveillance-automatisee-39818832.htm
Par @PierreCol

L’Enac s’engage pour la sécurité des vols de drones | Le Net Expert Informatique

	L’Enac s’engage pour la sécurité des vols de drones

La sécurité des vols de drones est prise très au sérieux par les instituts de recherche. L'Ecole nationale de l'Aviation civile (Enac) s'engage pour le progrès des systèmes de détection.
Gautier Hattenberger est l'un des six enseignants-chercheurs du laboratoire de recherche sur les drones, à la célèbre Enac, l'École nationale de l'aviation civile de Toulouse. Dans son labo, créé en 2005, il conçoit des machines, et enseigne la conception des drones à des élèves ingénieurs.

Comment percevez-vous l'émergence des drones civils, de plus en plus à la mode et désormais à la portée de tous ?
Au début de notre laboratoire, en 2005, les drones étaient encore très compliqués à construire, à concevoir. Il n'y avait que des avions dits de «modélisme», qui nécessitent des pistes et beaucoup d'espace pour voler. Vers 2008, certaines pièces électroniques ont atteint des tailles tellement petites, que les drones télé commandés sont devenus plus légers, plus faciles à piloter. Et les drones à décollage vertical, avec leurs rotors multiples, se sont développés. En gros, aujourd'hui, l'électronique fait presque tout, notamment dans les phases de décollage et d'atterrissage.

Les drones se sont retrouvés au centre de l'actualité : survols de centrales nucléaires, d'une école juive à Toulouse, de certains quartiers de Paris. Est-il possible de détecter rapidement le pilote de ces engins ?
Les systèmes actuels sont en phase de développement. L'Enac a d'ailleurs répondu à un appel à projets de l'Agence nationale pour la recherche, pour participer au développement de systèmes, qui pourront être radars, thermiques, sonores. Nous pourrions participer à une telle expérience en simulant une incursion de drone. Cet appel à projets montre bien que les autorités prennent très au sérieux la menace potentielle que peut représenter un drone mal utilisé.

Quelle est la réglementation actuelle pour faire voler un drone ?
Elle est très stricte et encadrée par la Direction générale de l'aviation civile. En gros, il faut beaucoup d'autorisations et d'habilitations. Le survol des zones habitées est interdit. Les opérateurs doivent figurer sur une liste qui mentionne notamment la nature de l'activité, le scénario de mission, le constructeur et le modèle de drone utilisé. Les pilotes doivent avoir obtenu une certification officielle et disposer d'une déclaration de niveau de compétence. Les autorisations de vol passent par le dépôt préalable auprès de la préfecture.

Des élèves spécialistes
Dès la rentrée prochaine, les élèves en cursus «ingénieur» à l'École nationale de l'aviation civile (Enac) suivront des cours dédiés spécifiquement aux drones. Le cursus actuel permet déjà aux élèves d'appréhender cette technologie, mais la formation à venir sera encore plus poussée. Elle permettra notamment aux élèves d'intégrer les sociétés conceptrices de drones, comme cela a déjà été le cas pour un élève de l'Enac, engagé par la société toulousaine Delair Tech à sa sortie de l'école.

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

Source : http://www.ladepeche.fr/article/2015/04/30/2096784-enac-engage-securite-vols-drones.html

Des pirates informatiques volent 5 millions de dollars à Ryanair | Le Net Expert Informatique

Des pirates informatiques volent 5 millions de dollars à Ryanair

Un peu moins de 5 millions de dollars (4,5 millions d'euros) ont été dérobés d'un des comptes de la compagnie aérienne à bas coûts Ryanair. Selon la société irlandaise, des pirates informatiques se seraient emparés de la somme par « un transfert électronique frauduleux passé via une banque chinoise ».

La compagnie travaille actuellement avec ses établissements bancaires et les autorités compétentes afin de récupérer ces fonds. Elle annonce dans un communiqué, publié mercredi 29 avril, que ceux-ci ont été « bloqués » et que des mesures ont été prises pour sécuriser les comptes de Ryanair. L'identité des pirates est encore inconnue.

Facture de kérosène

La société, dont le siège est à Dublin, assure des liaisons principalement en Europe. La plupart de ses transactions sont effectuées en euros, mais elle dispose aussi de comptes en dollars. D'après The Irish Times, les fonds en dollars ciblés par les pirates informatiques étaient destinés à payer ses factures de kérosène.

Le quotidien ajoute que l'agence judiciaire chargée du dossier en Irlande, le Criminal Assets Bureau (« bureau des biens d'origine criminelle ») de Dublin, avait pu identifier où la somme subtilisée avait été transférée grâce à un système de coopération internationale avec des agences jumelles en Asie.

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

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

Source : http://www.lemonde.fr/pixels/article/2015/04/29/des-pirates-informatiques-volent-5-millions-de-dollars-a-ryanair_4625234_4408996.html#Zc4r8duqZpt2kWJo.99

Multiplication des plaintes auprès de la CNIL | Le Net

Expert Informatique

Multiplication des plaintes auprès de la CNIL

Refus de déréférencement par Google, vidéosurveillance excessive dans le milieu du travail, radiation des fichiers bancaires… Le nombre de plaintes déposées auprès de la Cnil augmente et concernent surtout les données personnelles visibles sur internet selon son 35è rapport d'activité 2014 publié le 18 avril.

Soucieux de protéger leur vie privée et surtout leurs données personnelles, les particuliers n'hésitent plus à saisir la Commission pour exercer leur droit d'opposition à figurer dans un fichier. 5 825 plaintes ont ainsi été recensées en 2014, un chiffre en augmentation de 3 % par rapport à 2013.
La Commission a par ailleurs traité plus de 2 200 plaintes motivées par un problème d'e-réputation : suppression de textes, photographies, vidéos, coordonnées, commentaires, faux profils en ligne ou encore à prévenir la réutilisation de données publiquement accessibles sur internet.
Depuis l'instauration d'un « droit à l'oubli » par la CJUE, 200 plaintes ont été déposées suite à des refus de déréférencement de la part des moteurs de recherche.
Parmi les exemples cités par la Cnil, on retrouve celui d'une internaute qui, après avoir tapé ses nom et prénom sur un moteur de recherche, a constaté qu'ils renvoient vers des sites pornographiques. Sa demande de déréférencement lui a été refusée dans un premier temps, avant d'être acceptée suite à son intervention.
Un autre sujet d'importance qui a retenu l'attention de la Commission est la géolocalisation ou la vidéosurveillance en milieu professionnel qui, à elle seule, a fait l'objet de 300 dossiers en 2014. Suivent les plaintes motivées par la contestation de l'inscription au fichier national des incidents de remboursement des crédits aux particuliers ou au fichier central des chèques et des retraits de cartes bancaires.
Outre internet, 16 % des plaintes concernent le commerce, et notamment les problèmes liés à la radiation de fichiers publicitaires, à la conservation des coordonnées bancaires, aux fichiers clients et à la possibilité de s'opposer à la réception des courriels publicitaires.

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

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

Source : http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/126183/Multiplication-des-plaintes-aupres-de-la-CNIL.aspx
Par Lionel Costes

| Le Net Expert Informatique

Découvrez les pratiques des adolescents sur Internet et les médias sociaux | Le Net Expert Informatique

22

La Revue Française des SIC publie une étude qui analyse les relations entre les usages, notamment en termes d'accès à l'information, et les étapes de la vie adolescente. Les auteurs relèvent à la fois le rôle majeur joué par les réseaux sociaux en matière relationnelle mais aussi les pratiques offensantes inhérentes à l'immersion des adolescents dans l'univers des réseaux sociaux.

L'article de la Revue Française des Sciences de l'Information et de la Communication (RFSIC) prend appui sur certains des résultats de l'étude JAMES (Jeunes/Activité/Médias/Enquête suisse) menée en 2012, en partenariat avec les Universités de Zürich, de Lugano et de Genève.

Cette enquête visait à mesurer les usages des médias et réseaux sociaux par les adolescents et, à l'échelle suisse, à combler un manque en matière de recherche sur les pratiques médiatiques des adolescents.

Les auteurs du présent article s'appuient notamment sur un questionnaire fermé et standardisé, soumis à un échantillon de 1169 élèves âgés de 12 à 19 ans, et fréquentant des écoles (écoles de commerce, collèges) ou établissements professionnels (places d'apprentissage).

Usages des médias chez les adolescents

L'étude relève que les « 15-19 ans » ne sont que 16 % en France à lire la presse (gratuite et payante) tous les jours en 2009. Par comparaison, ils sont en Suisse, en 2012, plus de 50 % (58 % entre 16 et 19 ans) à le faire tous les jours ou plusieurs fois par semaine.

Concernant les garçons et leur attrait pour les jeux vidéo, on constate que cette pratique diminue dès « 14-15 ans », lorsque l'adolescent s'investit dans d'autres activités, notamment les sorties et les relations avec ses pairs sur les réseaux sociaux.

Ce phénomène de transfert, qui n'exclut pas selon l'étude des pratiques multitâches (35 % des adolescents parviennent par exemple à écouter ou à regarder la télévision en naviguant sur internet), s'observe également dans les pratiques lectorales avec une baisse d'intérêt pour la lecture de livres. Pour l'adolescent, la lecture de livres et de revues, contrairement au temps passé sur les réseaux sociaux, n'est pas perçue comme un moyen de reconnaissance relationnelle.

La lecture de la presse gratuite reste toutefois une pratique régulière : à partir de 16 ans, la presse, principalement gratuite, bénéficie d'un regain d'intérêt (36 % de lecteurs réguliers avant 16 ans, mais 55 % à 58 % des adolescents sont des lecteurs réguliers de la presse papier).

Dès 18 ans, la conversion vers la lecture des journaux en ligne devient significative, puisque 29 % des « 18-19 ans » lisent tous les jours ou plusieurs fois par semaine des quotidiens sur le Net. Les médias traditionnels ne sont pas ignorés dans ce contexte puisqu'un adolescent sur deux continue d'écouter régulièrement la radio, alors que 70 % à 80 % d'entre eux, selon leur âge, continuent à regarder la télévision tous les jours ou presque.

Pratiques informationnelles des adolescents

La large utilisation des smartphones chez les jeunes favorise le développement des pratiques informationnelles sur Internet et sur le Web 2.0, notamment l'usage des réseaux sociaux et des moteurs de recherche, moyens privilégiés de recherche d'informations.

Facebook et Instagram sont les deux sites attirant le plus de souscripteurs.

La variation la plus prononcée du taux d'adhésion à Facebook , précisent les auteurs, se situe à 14 ans, âge charnière, puisque d'un taux d'usage régulier de 59 % chez les « 12-13 ans » on passe à 86 % pour les « 14-15 ans ». Les sites de réseaux sociaux favorisent l'interlocution et les échanges synchroniques.

L'étude indique que « l'adolescent apparaît comme un individu en état de veille quotidien, observateur et évaluateur des profils de ses amis, qui entend contrôler son environnement immédiat ». Les réseaux sociaux sont aussi, parfois, le lieu d'expériences négatives en ligne.

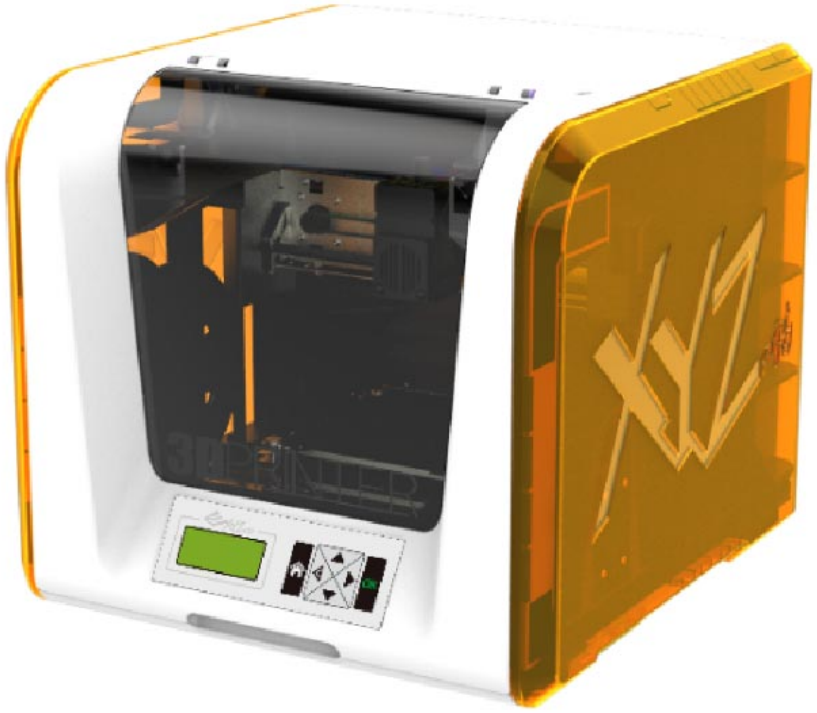
Les réseaux sociaux ou les forums sont en effet des plateformes potentiellement propices aux dérapages. Les propos délictueux et les agressions verbales sont fréquents sur les plateformes où on peut agir anonymement, sans s'exposer aux regards des autres, et disparaître en un clic de souris. Les agressions dont peuvent être victimes les adolescents (notamment la tranche d'âge des 16-17 ans) sont de plusieurs types : la diffusion d'informations fausses ou de propos offensants, la menace, la publication en ligne de photographies ou de vidéos sans autorisation de la personne concernée.

Ces outils, conclut l'étude, « se conçoivent alors aisément comme des espaces de rituels initiatiques et des territoires d'expérience, par lesquels les adolescents apprennent, par essais et erreurs, à négocier leur réputation en ligne et à gérer des données personnelles qui peuvent circuler à leur insu ».

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

Source : http://www.ludovia.com/2015/04/pratiques-des-adolescents-sur-internet-et-les-medias-sociaux/
Par Aurélie Julien

Une imprimante 3D à moins de 400€ en France? | Le Net Expert Informatique



Une imprimante 3D à moins de 400€ en France?

Les premières imprimantes 3D grand public débarquent en EuropeXYZprinting, concepteur primé pour la première gamme d'imprimantes 3D personnelles du marché, lance aujourd'hui trois nouveaux modèles en Europe. Destinées au grand public, aux entreprises et aux écoles du monde entier, les da Vinci Junior, da Vinci 1.1 Plus et Nobel 1.0 mettent l'impression 3D à la portée d'un large public de par leur facilité d'usage et leur prix abordable.
XYZprinting est un fabricant d'imprimantes 3D taïwanais adossé au fabricant mondial de matériel électronique New Kinpo Group, leader mondial sur le marché des matériels électroniques. Fort de plus de quinze années d'expérience dans le développement et la fabrication d'imprimantes dédiées à un usage personnel ou professionnel, New Kinpo Group génère un chiffre d'affaires annuel de plus 30 milliards de dollars et compte plus de 8 500 ingénieurs en R&D. XYZprinting dispose ainsi de bureaux à Taïwan, en Chine, au Japon, en Corée, aux Etats-Unis et en Europe.
Chacune des trois nouvelles imprimantes 3D donne accès à une très large palette de modèles 3D personnalisables référencés dans la bibliothèque Cloud de XYZprinting. Lors des grandes impressions, la maintenance est quant à elle réduite au minimum, grâce à la technologie de remplissage intégrée. Un détecteur intelligent surveille le niveau du bac et le recharge afin d'éviter les soucis de réapprovisionnement. Une fonctionnalité synonyme de gain : de temps, de consommables et d'argent. Avec ces nouveaux modèles, XYZprinting met l'impression 3D à la portée de tous les foyers, pour le coût d'une imprimante classique et sans nécessiter d'expérience ou de connaissances particulières.

da Vinci Junior
Dédiée à un usage personnel car très simple d'emploi, la da Vinci Junior est l'imprimante 3D la moins chère au monde. Disponible au prix de 399 € TTC, ce modèle compact est entièrement prêt à l'emploi. Cela en fait l'outil idéal pour les utilisateurs novices, les amateurs et les établissements scolaires. Très facile à utiliser, l'imprimante dispose d'un lecteur de carte SD intégré, ce qui lui permet éventuellement de se passer d'un ordinateur. La da Vinci Junior est équipée de la technologie FFF (Fused Filament Fabrication) : le filament en plastique PLA fondu transite par une buse et forme les différentes couches qui composeront l'objet imprimé.
Impression d'objets mesurant jusqu'à 150 x 150 x 150 mm
Poids : 12 kg
Une imprimante parmi les plus respectueuses de l'environnement : consommation de seulement 75 W pendant l'impression et utilisation de matériaux composés de plastique PLA biodégradable
Prix : 399 € TTC

Si vous le souhaitez, merci de nous faire part de vos impressions, critiques ou suggestions…

Source : http://www.capcampus.com/high-tech-1437/trouver-une-imprimante-3d-a-moins-de-400euros-en-france-a35099.htm

L’Afrique, le ventre mou de la lutte contre la cybercriminalité | Le Net Expert Informatique

	L’Afrique, le ventre mou de la lutte contre la cybercriminalité

Sous nos latitudes, les informations faisant état d'attaques criminelles contre telle ou telle autre institution publique ou privée passent quasi inaperçues. Au demeurant, elles n'intéressent qu'un petit groupe d'initiés attentifs aux questions de cybersécurité. Ces dernières années, des attaques informatiques gravissimes se sont déroulées presque dans tous les pays africains, mais sans vraiment émouvoir grand monde.

Pourtant, nous devrions prêter davantage d'attention à ces attaques qui sont autant de coups portés à l'intégrité voire à la souveraineté de nos entreprises, de nos institutions et de nos Etats. Au Burkina Faso, un communiqué du Ministère du Développement de l'Economie numérique et des Postes, rendu public le 23 avril 2015, annonçait que les sites institutionnels du Burkina avaient été victimes de cyber-attaques.
Le communiqué précisait que « les techniciens de l'Agence nationale de promotion des technologies de l'information et de la communication se sont mis à pied d'œuvre en collaboration avec d'autres services techniques notamment l'Agence nationale de sécurité des systèmes d'informations (ANSSI) pour circonscrire l'attaque et rétablir dans les meilleurs délais les différents sites web des ministères et institutions ».
Le weekend d'avant, c'est le site internet de la très respectable Présidence de la République du Mali qui faisait l'objet d'attaques de hackers dont nous imaginons qu'ils n'ont jamais été identifiés. Le CM du compte a eu l'obligeance d'avertir le public en publiant quelques tweets, le samedi 18 avril dernier, sur le fil de @PresidenceMali :
MALI | Notre site internet koulouba.ml est attaqué depuis hier soir. Nos services techniques sont à pied d'œuvre pour résoudre le problème 1/2
MALI | Nous présentons nos excuses aux usagers qui étaient supposés lire hier soir le Communiqué du Conseil des Ministres via un lien 2/2
MALI | Le site de la Présidence de la République à nouveau opérationnel grâce à l'expertise de nos collègues du Service Informatique #SINTI

L'AGETIC, notre « firewall » national a-t-elle seulement appris la nouvelle de l'intrusion de petits malins dans le saint des saints ? Si oui, qu'a-t-elle fait pour « contre-hacker » les indésirables petits intrus ? Pas grand-chose, je suppose ! Sans nulle volonté de semer quelque peur-panique, nous rappelons que, déjà en janvier 2015, le site de l'Agence de l'informatique de l'Etat (ADIE, rattachée à la présidence) a publiquement reconnu avoir subi une série d'attaques informatiques dont les auteurs seraient des hackers pro Charlie-Hebdo.
Le Nigéria est aussi régulièrement cité comme une terre de prédilection des hackers qui ne se privent pas de profiter du grand désordre ambiant. On pourrait multiplier les exemples à l'infini sans que, nous en avons l'intime conviction, notre alerte n'incite les décideurs à investir massivement dans la protection de nos architectures informatiques. Mais, touchons du bois, le réveil pourrait être un jour douloureux d'autant plus que les hackers les plus virulents connus à ce jour seraient africains.
Nous n'avons malheureusement aucun indicateur pour vérifier la réalité de cette information, mais c'est le signal que, la mondialisation aidant, nos jeunes deviennent aussi des petits monstres abreuvés à la source du désespoir et du manque de perspective. Les spécialistes des questions de cybersécurité localisent ces nouveaux fous furieux du web dans les pays du Maghreb, en particulier au Maroc et en Algérie où l'idéologie salafiste a formaté de nombreuses têtes malheureusement bien faites, prêtes à porter le coup de grâce au modèle occidental.
Dans le lot, un nom émerge : Hamza Bendellaj. Il est algérien et n'a que 24 ans, mais bénéficie déjà d'une réputation sulfureuse. Appelé le « hacker riant », il a été arrêté par le FBI le 6 janvier 2013 à Bangkok, alors qu'il transitait par l'aéroport Suvarnabhumi en provenance de Malaisie. Ce jeune Algérien aurait piraté des comptes privés dans 217 banques à travers le monde et, au passage, empoché entre « 10 et 20 millions de dollars ».

Si vous le souhaitez, merci de nous faire part de vos impressions, critiques ou suggestions…

Source : http://malijet.com/actualite_internationale/128190-chronique-du-web-l%E2%80%99afrique,-le-ventre-mou-de-la-lutte-contre-la-.html
Par Serge de MERIDIO