La vente liée d’un OS et d’un PC est elle illégale en Europe ?

La vente liée d’un OS et d’un PC est elle illégale en Europe ?

La Cour de justice de l'Union tranche un conflit opposant un consommateur à Sony dans la vente groupée d'un PC et de Windows. Et valide les pratiques des constructeurs.

La fin d'un long feuilleton ? Cela y ressemble fort. La Cour de justice de l'Union européenne (CJUE) vient en effet d'estimer que la vente d'un ordinateur équipé de logiciels préinstallés « *ne constitue pas, en soi, une pratique commerciale déloyale* ». Cet avis vient trancher une affaire qui a débuté en France en 2008. Au centre des débats : la vente de logiciels – en l'espèce Windows Vista et autres applications – à un PC de marque Sony. Le consommateur qui est à l'origine de l'affaire refuse la pratique imposée par le marché et demande le remboursement des logiciels préinstallés à Sony.
Devant le refus du constructeur, l'affaire est portée en justice par l'utilisateur, qui y voit une pratique commerciale déloyale. Saisie *in fine* de l'affaire, la Cour de cassation demande à la CJUE de statuer sur deux points. Primo, l'absence d'alternative proposée au consommateur (soit le même ordinateur vendu nu) est-elle une pratique commerciale déloyale ? Secundo, une offre groupée – PC + logiciels donc – doit-elle faire obligatoirement apparaître le prix de chacune de ses composantes ?…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : La vente liée d'un OS et d'un PC n'est pas illégale en Europe

Sécurité informatique des collectivités : Toujours plus avec moins…

Sécurité informatique des collectivités : Toujours plus avec moins…

Les collectivités et leurs groupements, notamment les communautés de communes, peinent encore à prendre en compte tous les aspects de la sécurité des systèmes d'information, à en croire le rapport 2016 du Club de la sécurité de l'information Français (Clusif). Alors qu'elles se numérisent de plus en plus, les collectivités vont devoir maintenir voire accentuer leurs efforts dans un contexte budgétairement contraint.

Dans l'édition 2016 de son rapport sur les « Menaces informatiques et pratiques de sécurité en France » (Mips), le Club de la sécurité de l'information Français (Clusif) se penche de nouveau sur les collectivités (1). De plus en plus nombreuses à recourir à des services dématérialisés, celles-ci auront à charge de « maintenir » leurs « efforts » pour « assurer la sécurité de leur système d'information et des informations qui leur sont confiées », selon les auteurs de ce document de plus de cent pages. Le tout dans un contexte budgétaire restreint. Globalement, alors que le sentiment de dépendance à l'égard du numérique s'enracine, la sécurité des systèmes d'information est « efficiente dès lors que les moyens organisationnels, humains et financiers sont clairement attribués » et que la direction est fortement impliquée, indique le rapport. Cependant, sur la base des 203 collectivités interrogées, il est fait état de grandes disparités entre les échelons territoriaux, où les communautés de communes sont à la peine.

Stagnation des budgets malgré la numérisation en cours

Publié tous les deux ans, le « Mips » délivre un bilan approfondi des usages en matière de sécurité de l'information ; et inclut dans son édition 2016 (comme tous les 4 ans) les collectivités territoriales de grande taille. Autrement dit les communes de plus de 30.000 habitants, les intercommunalités (communautés de communes, d'agglomération, communautés urbaines ou encore les métropoles) et enfin les régions et les départements (regroupés par le rapport sous le terme de conseils territoriaux).

Côté résultats, si une grande partie des collectivités interrogées a confié un sentiment toujours croissant de « dépendance » vis-à-vis de l'informatique (75% contre 68% en 2012), les budgets qui y sont liés tendent pourtant à baisser et restent très disparates (avec un rapport de 1 à 100 entre les plus petits et les plus importants). Ainsi, près de 54% des collectivités ont un budget informatique inférieur à 100.000 euros en 2016, contre 45% en 2012. En moyenne, les conseils territoriaux sont les mieux dotés avec 5,8 millions d'euros, pour un million d'euros dans les intercommunalités et 800.000 euros dans les villes.

Dans ce total, la part de la sécurité est difficilement évaluable et demeure au mieux constante (67% des cas) ou diminue (28% des collectivités contre 14% en 2012 y consacrent moins de 1% de leur budget informatique). Enfin, si augmentations il y a, elles servent avant tout à mettre en place des solutions de sécurité (25%), même si des efforts importants sont effectués en matière organisationnelle (11%) et en sensibilisation (9%).

Pas de politique de sécurité sans personnels qualifiés

Bien que majeur, l'aspect financier n'occupe que la deuxième place des principaux freins pour les collectivités (à 45%), pour qui l'absence de personnels qualifiés semble être le véritable problème (à 47%), accru par un manque avoué de connaissance (38%). En conséquence, les contraintes organisationnelles (29%) et les réticences de la direction générale, des métiers ou des utilisateurs (24%) ferment la marche.

Malgré tout, l'étude montre que les collectivités sont de plus en plus nombreuses à formaliser leur politique de sécurité (PSI), en particulier les villes (54% contre 43% en 2012) et les conseils territoriaux (52% contre 35%). A l'inverse, les communautés de communes sont à la peine (un peu plus de 2 sur 10).

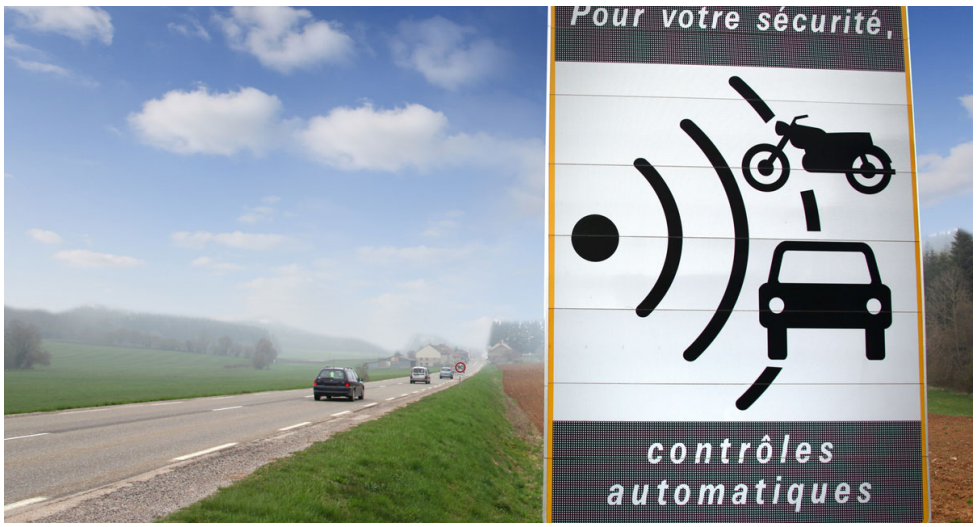
Concrètement, les DSI (directions des systèmes d'information) gèrent les politiques de sécurité dans 65% des cas, alors que les directions générales des services tendent à se désengager (impliquées dans 54% des cas, contre 80% en 2012). Dans 21% des cas, des élus y ont contribué. Enfin, on notera que la présence d'un responsable de la sécurité des systèmes d'information (RSSI) « serait une condition sine qua none pour disposer d'une PSI ». Par ailleurs de plus en plus nombreux (+3 points, à 35%), les RSSI voient cependant leur fonction se diluer, avec 39% de personnel dédié en 2016 contre 62% en 2012 dans les villes, pour ne citer qu'elles. Enfin, ils sont bien souvent rattachés à la DGS (dans les communautés de communes notamment) ou à la DSI (dans les régions ou les départements par exemple) – selon une règle qui veut que « plus la collectivité est petite et plus les fonctions sont cumulées par le comité de direction »…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Sécurité informatique : les collectivités encouragées à maintenir leurs efforts – Localtis.info – Caisse des Dépôts

---

Est-ce que la cour de cassation a finalement jugé illégal le signalement des radars par Facebook ?



Est-ce que la cour de cassation a finalement jugé illégal le signalement des radars par Facebook ?

La cour de cassation a jugé que les pages Facebook sur lesquels les internautes s'informent de la localisation de contrôles de police sur les routes ne sont pas illégales au regard de l'état actuel du code pénal, qui interdit les avertisseurs radars.

Le fait d'utiliser un réseau social comme Facebook pour prévenir ses amis ou d'autres internautes de la géolocalisation de contrôles routiers et de radars automatiques n'est pas une violation de la loi pénale, a tranché cette semaine la cour de cassation, dont l'arrêt est cité par Le Figaro.

La haute juridiction s'était penchée sur la question à la demande du parquet de Montpellier, qui s'était pourvu en cassation après la décision de la cour d'appel de Montpellier de relaxer des individus qui avaient créé une page Facebook intitulée « *le groupe qui te dit où est la police en Aveyron* ».

Alors que la douzaine d'internautes avait été condamnée en première instance en décembre 2014, au motif que l'utilisation d'un tel groupe Facebook violerait le code de la route qui interdit les avertisseurs de radars depuis 2012, la cour de Montpellier avait adopté une lecture plus littérale de l'article R413-15 du code de la route, pour estimer que ça n'était pas la même chose.

UN RÉSEAU SOCIAL N'EST PAS UN DISPOSITIF D'AVERTISSEUR RADAR

Cet article interdit les « *dispositifs ou produits visant à avertir ou informer de la localisation d'appareils, instruments ou systèmes servant à la constatation des infractions à la législation ou à la réglementation de la circulation routière* ». Toute la question était de savoir si un groupe Facebook, ou équivalent, pouvait être assimilé à un « *dispositif visant à avertir ou informer de la localisation* » de contrôles de sécurité routière.

.La cour de cassation apporte une réponse claire puisqu'elle indique que « *l'utilisation d'un réseau social, tel Facebook, sur lequel les internautes inscrits échangent des informations, depuis un ordinateur ou un téléphone mobile, ne peut être considérée comme l'usage d'un dispositif de nature à se soustraire à la constatation des infractions relatives à la circulation routière incriminée par l'article R.413-15 du code de la route* ».

Peu importe, au final, que les internautes en question aient utilisé des messages cryptiques pour se faire comprendre (du genre « les poulets cuisent au soleil à 500 mètres du rond point »). Même s'ils avaient communiqué de façon très explicite, la loi ne l'interdit pas, au grand dam de la gendarmerie qui doit de temps en temps rappeler que signaler des contrôles routiers, c'est aussi aider des personnes recherchées qui peuvent être appréhendées par ce biais.

Nul doute, dès lors, que des propositions visant à compléter la loi devraient parvenir sur nos écrans dans les prochaines semaines ou les prochains mois.

Article de Guillaume Champeau

Réagissez à cet article

Original de l'article mis en page : Signaler des radars avec

Facebook ? La cour de cassation juge que c’est légal – Politique – Numerama

---

Directive NIS adoptée: quelles conséquences pour les entreprises?

Directive NIS depuis juillet. Des changements pour les entreprises?

En juillet dernier, le Parlement européen a adopté la directive NIS (Network and Information Security). Les opérateurs de services ainsi que les places de marché en ligne, les moteurs de recherche et les services Cloud seront soumis à des exigences de sécurité et de notification d'incidents.

C'est fait ! La directive NIS a été approuvée le 6 juillet par le Parlement européen en seconde lecture, après avoir été adoptée en mai dernier par le Conseil de l'Union européenne. Cette directive est destinée à assurer un « niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne ». Les « opérateurs de services essentiels » et certains fournisseurs de services numériques seront bien soumis à des exigences de sécurité et de notification d'incidents de sécurité.

Sécuriser les infrastructures

Du côté des fournisseurs de services numériques, les places de marché en ligne, les moteurs de recherche et les fournisseurs de services de Cloud actifs dans l'UE sont concernés. Ils devront prendre des mesures pour « assurer la sécurité de leur infrastructure » et signaler « les incidents majeurs » aux autorités nationales. Mais les exigences auxquelles devront se plier ces fournisseurs, seront moins élevées que celles applicables aux opérateurs de services essentiels.

Publication de la Directive NIS au Journal officiel de l'Union européenne
Adoption de la directive NIS : l'ANSSI, pilote de la transposition en France

---

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

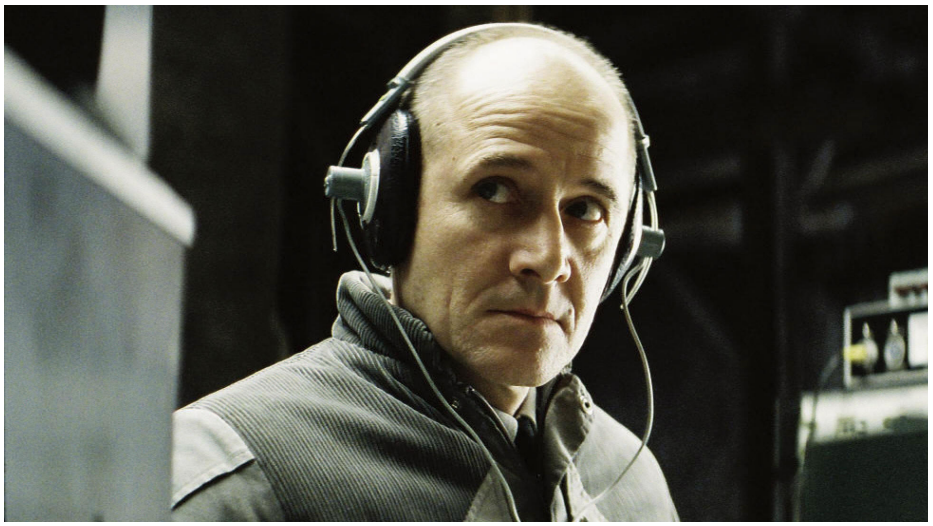
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Directive NIS adoptée: quelles conséquences pour les entreprises?

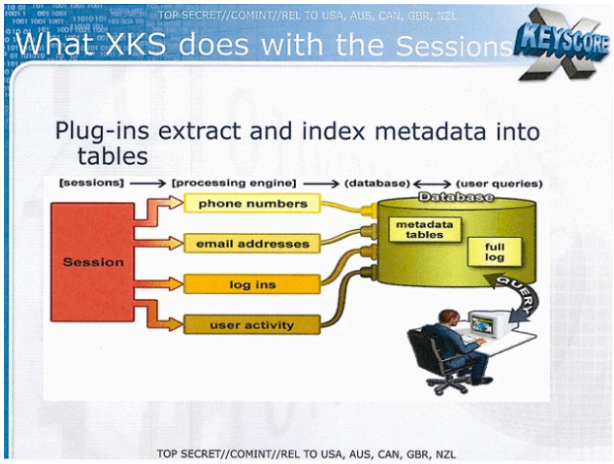
Collectes massives et illégales par le Renseignement allemand

	Collectes massives et illégales par le Renseignement allemand

---

Après avoir réalisé un contrôle sur place des services de renseignement, la Cnil allemande a dressé un bilan extrêmement critique des activités du Bundesnachrichtendienst (BND) en matière de collecte d'informations sur Internet.

Le site Netzpolitik a dévoilé le contenu d'un rapport jusque là confidentiel produit en juillet 2015 par Andrea Voßhoff, le commissaire à la protection des données en Allemagne, qui accable les services de renseignement allemands. Le rapport a été réalisé après la visite de l'homologue de la Cnil dans la station d'écoutes Bad Aibling, opérée conjointement en Bavière par l'agence allemande du renseignement, la Bundesnachrichtendienst (BND), et par la National Security Agency (NSA) américaine.
Malgré les difficultés à enquêter qu'il dénonce, Voßhoff dénombre dans son rapport 18 violations graves de la législation, et formule 12 réclamations formelles, qui obligent l'administration à répondre. Dans un pays encore meurtri par les souvenirs de la Stasi, le constat est violent.
L'institution reproche au BND d'avoir créé sept bases de données rassemblant des informations personnelles sur des suspects ou simples citoyens lambda, sans aucun mandat législatif pour ce faire, et de les avoir utilisées depuis plusieurs années au mépris total des principes de légalité. Le commissaire a exigé que ces bases de données soient détruites et rendues inutilisables.



Parmi elles figure une base assise sur le programme XKeyScore de la NSA, qui permet de réunir et fouiller l'ensemble des informations collectées sur le Web (visibles ou obtenues par interception du trafic), pour les rendre accessibles aux analystes qui veulent tout savoir d'un individu et de ses activités en ligne. Alors que XKeyScore est censé cibler des suspects, Voßhoff note que le programme collecte « un grand nombre de données personnelles de personnes irréprochables », et cite en exemple un cas qu'il a pu consulter, où « pour une personne ciblée, les données personnelles de quinze personnes irréprochables étaient collectées et stockées », sans aucun besoin pour l'enquête…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le Renseignement allemand pris en flagrant délit de collectes massives illégales – Politique – Numerama

Retrouver l’auteur d’un E-mail à partir de l’adresse IP : Le demandeur condamné

Retrouver l’auteur d’un E-mail à partir de l’adresse IP : Le demandeur condamné

Le TGI de Meaux a débouté l'entreprise qui voulait obtenir de Numericable les noms, prénoms, adresses et coordonnées complètes de l'auteur d'un email frauduleux à partir de son adresse IP.

Dans une ordonnance de référé du 10 août 2016 repérée par Legalis, le tribunal de grande instance de Meaux (Seine-et-Marne) a débouté l'entreprise qui voulait obtenir de Numericable les données d'identification correspondant à l'adresse IP de l'auteur présumé d'un email frauduleux.
Comment en est-on arrivé là ? En début d'année, la société France Sécurité a préparé une proposition commerciale à l'attention d'Airbus Helicopters dans le cadre d'un appel d'offres. Dans la foulée, le distributeur d'équipements de protection individuelle a reçu un courriel d'un individu se faisant passer pour un employé d'Airbus et lui demandant de transmettre par courriel le fichier contenant la proposition… Suspectant la fraude, France Sécurité a contacté Airbus. Le nom associé au courriel était bien celui d'un de ses employés, mais il n'était pas l'auteur des courriels en question.

Usurpation d'identité
Dans un premier temps, une plainte a été déposée contre X pour usurpation d'identité. Parallèlement, le département informatique de France Sécurité a identifié l'adresse IP de l'expéditeur du courriel (transmis via Gmail) ainsi que le FAI hôte, à savoir : Numericable. Un procès-verbal de constat d'huissier a été établi. Ensuite, le 28 juin 2016, France Sécurité a déposé plainte auprès du procureur de la République près le tribunal de grande instance de Nantes. Et le 8 juillet 2016, l'entreprise a fait assigner devant le juge des référés du TGI de Meaux le câblo-opérateur. Le but : obtenir du tribunal qu'il ordonne au FAI de communiquer dans un délai de 48 heures les données d'identification correspondant à l'adresse IP en cause. Car, selon le demandeur, le câblo-opérateur est tenu de conserver les données permettant l'identification de son client et de déférer aux demandes de l'autorité judiciaire. Et ce en application de la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004. France Sécurité souhaitait également qu'une astreinte soit versée par Numericable en cas de dépassement de ce délai, en plus des frais irrépétibles… Sans succès.

L'adresse IP, une donnée personnelle
Le juge est parti du principe que l'adresse IP est une donnée à caractère personnel. Par ailleurs, il a considéré que la collecte de cette donnée constitue un traitement au sens de la loi informatique et libertés. Une telle collecte aurait donc dû faire l'objet d'une autorisation de la Commission nationale informatique et libertés (Cnil) accordée à France Sécurité. Cela n'a pas été le cas. Par ailleurs, le juge considère que le cadre juridique applicable dans ce dossier ne peut pas être celui de la LCEN de 2004. Selon lui, Numericable n'est pas visé en tant que « personne dont l'activité est d'offrir un accès à des services de communication au public » en relation avec « la création d'un contenu » en ligne.
Résultat : le TGI de Meaux a débouté France Sécurité de toutes ses demandes. L'entreprise a été condamnée aux entiers dépens et au versement de 2 000 euros au titre des frais irrépétibles…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : IP : Numericable n’a pas à communiquer les données d’identification

---

Pokémon Go inquiète l’armée française !

Pokémon Go inquiète l’armée française !

Une note de la Direction de la protection des installations militaires explique en quoi le jeu Pokémon Go représente une menace pour les sites protégés du ministère de la Défense, et délivre des consignes pour interdire le jeu à proximité des zones concernées.

L'accès aux sites militaires est interdit – ou très restreint – au grand public. Et cela vaut également pour les Pokémon. Du moins c'est l'intention affichée par le ministère de la Défense dans une note dévoilée par Le Canard Enchaîné dans son numéro du 31 août (page 4).

Le document révélé date du 25 juillet et est en effet signé par le contre-amiral Frédéric Renaudeau, patron de la Direction de la protection des installations, moyens et activités de la Défense (DPID). On y apprend que plusieurs zones sensibles du ministère de la défense « *abriteraient ces objets et créatures virtuelles. Les risques d'intrusion ou d'attroupement à proximité immédiate sont réels* ».

TOUTE PRÉSENCE DE CRÉATURES ET D'OBJETS VIRTUELS À L'INTÉRIEUR DES ENCEINTES DEVRA ÊTRE SIGNALÉE

Le ton est grave et les risques de Pokémon Go sont fortement soulignés par le contre-amiral. Celui mentionne en effet plusieurs points qu'il juge très dangereux :

- *« sous couvert du jeu, il ne peut être exclu que des individus mal intentionnés cherchent à s'introduire subrepticement ou à recueillir des informations sur nos installations […] ;*
- *les données de géolocalisation des joueurs, non protégées, pourraient donner lieu à exploitation ;*
- *ce jeu peut générer des phénomènes addictifs préjudiciables à la sécurité individuelle et collective du personnel de la défense. »*

Pour contrer la menace, le contre-amiral a délivré des consignes strictes. Le Canard Enchaîné affirme ainsi que dans une annexe de la note, ce dernier interdit l'utilisation de l'application à l'intérieur et à proximité des sites militaires et demande à ce que les forces de sécurité intérieure soient alertées en cas d'attroupement sur la voie publique.

La conclusion de la note est sûrement l'élément le plus incongru. Il y est en effet précisé que « toute présence de créatures et d'objets virtuels à l'intérieur des enceintes » devra être signalée à la DPID. Grâce à cela, le document officiel estime que « cette cartographie permettra de consolider notre évaluation de la menace ».

Il est intéressant de voir à quel point le jeu Pokémon Go peut susciter les pires craintes des hautes sphères décisionnelles. Ici, on ne peut s'empêcher d'esquisser un sourire en lisant les termes un tantinet exagérés pour parler des dangers de l'application. On peut également dénoncer quelques paradoxes. En effet, comment signaler la présence d'une créature sur les sites concernés si l'utilisation de Pokémon Go est formellement interdite ?

On peut tout de même nuancer en estimant que le ton un brin catastrophique de la note est de rigueur pour tout ce qui touche à la sécurité intérieure, surtout dans le contexte actuel. À noter que, récemment, la ministre Najat Vallaud-Belkacem, a demandé rendez-vous avec Niantic pour retirer tous les Pokémon rares dans les établissements scolaires.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Quand Pokémon Go inquiète l'armée française – Pop culture – Numerama

---

La cybercriminalité a de

belles années devant elle

La cybercriminalité a de belles années devant elle

Les prochaines années laissent entrevoir de beaux moments pour les cybercriminels de tout acabit. Les raisons expliquant cela sont nombreuses. Quelles sont-elles?

Suivre la scène de la sécurité informatique a ceci de particulier : c'est à la fois fascinant et grandement décourageant. C'est d'autant plus décourageant que les tendances présentes au cours des derniers mois laissent entrevoir de beaux jours pour les cybercriminels. Essentiellement, quatre raisons expliquent cela.

La multiplication des cibles potentielles

La première raison est assez évidente : il y a de plus en plus de cibles disponibles pour les criminels. La surmultiplication du nombre de plateformes exploitant Internet a pour effet de toutes les transformer en des opportunités potentielles pour des gens malintentionnés. La manifestation la plus flagrante de cette surmultiplication se transpose dans la fulgurante montée de l'Internet des objets.
Ce nouvel eldorado porte toutefois les gènes de sa propre insécurité. En effet, le marché est meublé par une multitude de joueurs, et leur intérêt porté à la chose sécuritaire est tout aussi variable. Ainsi, alors que l'objectif est d'occuper le marché le plus rapidement possible, bon nombre de joueurs impliqués dans la course à l'Internet des objets arrivent sur le marché avec des produits qui sont, volontairement ou involontairement, plus ou moins sécurisés.
Bref, nous sommes placés devant un cercle vicieux duquel nous ne pouvons pas nous sortir : plus de technologies signifient nécessairement plus de vulnérabilités et, conséquemment, plus d'opportunités criminelles. De plus, croire que l'on puisse mettre un frein à l'évolution technologique est illusoire.

Le difficile marché de la sécurité

Le contexte actuel rend les ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés.
Alors que le domaine apparaît comme extrêmement complexe, le manque criant de main-d'œuvre est de plus en plus problématique dans les entreprises. Forbes affirme pourtant que ce secteur vaudra sous peu 75 milliards de dollars US et que le marché créera plus d'un million d'emplois.
Non seulement manque-t-il de spécialistes en sécurité, mais il manque aussi de plus en plus de pirates black hat sur le marché, faisant en sorte que les cybercriminels eux-mêmes se tournent de plus en plus vers des modèles de sous-traitance pour effectuer leurs opérations.
Ce manque d'expertise a pour effet de rendre l'économie globalement plus ou moins axée sur la sécurité. Certes, certains secteurs ont les moyens de leurs ambitions, mais le contexte actuel rend ces ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés. Les effets sont bien sûr conséquents : la situation engendre une sécurité bien inégale, avec le lot de vulnérabilités qu'elle impose.

La rentabilité évidente

Autre point extrêmement important pour expliquer pourquoi la cybercriminalité aura le vent dans les voiles? C'est lucratif. La logique criminelle est relativement simple : il s'agit de faire le plus d'argent possible, le plus facilement possible. En somme, c'est le capitalisme en action.
Dans le domaine de la cybercriminalité, cela fonctionne décidément. On estime à 445 milliards de dollars US le marché de la cybercriminalité. Bon, je vous entends déjà geindre et dire que c'est fort de café. Soit. Admettons que ce soit la moitié moins, c'est tout de même 222 milliards, batinse!
Pour rappel, le budget du Canada est d'environ 290 milliards de dollars CA. C'est donc payant, et c'est bien dommage, mais les conséquences de la cybercriminalité sont minimes. Les chances d'arrêter les criminels sont plutôt basses (voir point suivant) et les peines encourues ne sont pas adaptées.

L'incapacité d'action des agences d'application de la loi

Les cybercriminels ont donc le beau jeu, puisque le risque de se faire prendre est extrêmement bas. En effet, les forces policières sont mal équipées pour confronter la cybercriminalité, faisant en sorte que trop souvent, elles doivent capituler devant les actions commises par les criminels. Dans les cas les plus extrêmes, les agences tenteront de déployer les efforts nécessaires pour faire culminer une enquête, mais cela se fera à grands coups de contrats avec le secteur privé afin de se procurer l'expertise nécessaire pour résoudre le crime en question. Le fait que le FBI ait versé un montant de 1,3 million à un groupe de «chercheurs en sécurité», considérés par plusieurs comme ayant des mœurs on ne peut plus douteuses, pour accéder aux données présentes dans l'iPhone du terroriste de San Bernardino en est, en soi, la manifestation la plus éloquente.
Lutter contre la cybercriminalité demande essentiellement quatre choses. Une culture particulière, une collaboration internationale, des moyens et des techniques disponibles, et des compétences de pointe dans le domaine des technologies. Le dur constat qu'il faut faire, c'est qu'outre la collaboration internationale, les autorités compétentes n'ont pas les moyens pour atteindre les trois autres prérequis. Par conséquent, la vaste majorité des corps policiers ne s'attaqueront aux cybercrimes que lorsque les infractions sont trop exagérées.

La somme de toutes les peurs

Au final, ce qui est le plus inquiétant dans cette situation, c'est que plus le temps avance, plus les réseaux de cybercriminels deviennent solides, sophistiqués et ont de plus en plus de moyens. Les laisser agir en toute impunité a pour effet de les rendre toujours plus coriaces, ce qui rendra la tâche de lutter contre eux d'autant plus difficile à long terme. Il faudra que l'on prenne le problème à bras le corps une fois pour toute, sinon, nous risquons d'avoir de mauvaises surprises dans les prochaines années.
Article original de branchez-vous.com

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : La cybercriminalité a de belles années devant elle | Branchez-vous

---

Où en est la protection des lanceurs d’alerte ?

	Où en est la protection des lanceurs d’alerte ?

Lanceurs d'alerte : nullité du licenciement d'un salarié ayant dénoncé de bonne foi des faits susceptibles de recevoir une qualification pénale.
Pour la première fois, par un arrêt du 30 juin 2016 (n°15-10.557), la Cour de cassation s'est prononcée sur la sanction du licenciement d'un salarié lanceur d'alerte.
Dans cette affaire, le directeur administratif et financier d'une association qui assurait la gestion d'un centre d'examen de santé avait été licencié pour faute lourde en mars 2011 après avoir dénoncé auprès du procureur de la République des faits susceptibles de constituer une escroquerie et un détournement de fonds de la part d'un membre du conseil d'administration et du président de l'association.
(Cass. Soc. 30 juin 2016, n°15-10.557)

1) La nullité du licenciement du salarié lanceur d'alerte prononcé en violation de la liberté d'expression
A l'époque des faits donc, la loi n°2013-1117 du 6 décembre 2013 qui prévoit que le licenciement d'un salarié fondé sur le fait qu'il témoigne ou dénonce, de bonne foi, des faits susceptibles de recevoir une qualification pénale est nul, n'était donc pas applicable.
Aussi, la cour d'appel avait estimé que le licenciement du directeur administratif et financier était certes dépourvu de cause réelle et sérieuse puisqu'il avait dénoncé les faits en parfaite bonne foi, mais elle avait refusé de prononcer la nullité du licenciement.
La cour d'appel avait ainsi fait une stricte application de la règle selon laquelle il n'y a « pas de nullité sans texte » hors les cas d'atteinte à une liberté fondamentale et avait relevé la loi du 6 décembre 2013 n'était pas applicable au moment des faits.
Pourtant, la chambre sociale, saisie d'un pourvoi formé par le salarié contre cette décision, a estimé, au visa de l'article 10§1 de la Convention européenne des droits de l'Homme, que le licenciement du lanceur d'alerte était nul car prononcé en violation de la liberté d'expression :
« Vu l'article 10 § 1 de la de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ;
Attendu qu'en raison de l'atteinte qu'il porte à la liberté d'expression, en particulier au droit pour les salariés de signaler les conduites ou actes illicites constatés par eux sur leur lieu de travail, le licenciement d'un salarié prononcé pour avoir relaté ou témoigné, de bonne foi, de faits dont il a eu connaissance dans l'exercice de ses fonctions et qui, s'ils étaient établis, seraient de nature à caractériser des infractions pénales, est frappé de nullité ;
Attendu que pour dire qu'il n'y avait pas lieu d'annuler le licenciement et débouter le salarié de sa demande de réintégration, l'arrêt retient que la nullité ne peut être prononcée en l'absence de texte la prévoyant puisque les articles L. 1132-3-3 et L. 1132-4 du code du travail issus de la loi n° 2013-1117 du 6 décembre 2013, n'étaient pas applicables à l'époque du licenciement et que les faits dénoncés par le salarié ne se rattachaient pas à des faits de corruption, ce qui exclut l'application de l'article L. 1161-1 du code du travail ;
Qu'en statuant ainsi, alors qu'elle avait constaté que le licenciement était motivé par le fait que le salarié, dont la bonne foi ne pouvait être mise en doute, avait dénoncé au procureur de la République des faits pouvant être qualifiés de délictueux commis au sein de l'association, la cour d'appel qui n'a pas tiré les conséquences légales de ses constatations, a violé le texte susvisé. »
Ce faisant, la chambre sociale de la Cour de cassation se conforme à l'approche adoptée par la Cour européenne des droits de l'Homme (*CEDH, 12 février 2008, Guja c. Moldova, n°14277/04*).

2) Une protection contre le licenciement conditionnée à la seule bonne foi du lanceur d'alerte
La nullité du licenciement est toutefois soumise à la condition que le salarié qui a dénoncé des faits susceptibles de recevoir une qualification pénale l'ait fait de bonne foi.
La bonne foi doit ici être interprétée comme la croyance légitime du salarié en la commission desdits faits.
Aussi, le salarié qui dénoncerait une infraction pénale de manière parfaitement mensongère simplement pour se protéger d'un licenciement qu'il sentirait approcher, ne pourrait pas bénéficier de cette solution.
En revanche, la protection s'appliquerait à un salarié qui dénonce de bonne foi des faits susceptibles de recevoir une qualification pénale même s'il s'avère ensuite que le salarié s'est trompé et qu'aucune infraction n'a finalement été commise.
En effet, l'attendu de principe de l'arrêt du 30 juin 2016 ne laisse aucune place au doute à cet égard puisqu'il est formulé ainsi :
« *Attendu qu'en raison de l'atteinte qu'il porte à la liberté d'expression, en particulier au droit pour les salariés de signaler les conduites ou actes illicites constatés par eux sur leur lieu de travail, le licenciement d'un salarié prononcé pour avoir relaté ou témoigné, **de bonne foi**, de faits dont il a eu connaissance dans l'exercice de ses fonctions et qui, s'ils étaient établis, seraient de nature à caractériser des infractions pénales, est frappé de nullité* ; »
En outre, par cet arrêt la chambre sociale va encore plus loin que son homologue européen puisque contrairement à la Cour européenne des droits de l'Homme, elle ne fait aucune référence à l'intérêt général comme condition d'application de la protection.
Enfin, la chambre sociale ne subordonne pas non plus le bénéfice de cette protection à la nécessité de respecter la graduation de la procédure d'alerte. En effet, pour la Cour de cassation, peu importe que le salarié ait averti sa hiérarchie préalablement à la dénonciation auprès de l'autorité judiciaire ou qu'il ait directement informé le procureur de la République.
De même, si en l'espèce, le directeur administratif et financier avait porté sa dénonciation auprès du procureur de la République, la Cour de cassation, dans son communiqué relatif à l'arrêt, précise que : *« Une telle décision est de nature à protéger les lanceurs d'alerte, dans la mesure où, la chambre sociale instaure cette immunité non seulement lorsque les faits sont portés à la connaissance du procureur de la République mais également, de façon plus générale, dès lors qu'ils sont dénoncés à des tiers ».*
Par cette décision, la Cour de cassation consacre donc la solution retenue par le législateur dans la loi du 6 décembre 2013 et étend ainsi la protection contre le licenciement à l'ensemble des lanceurs d'alerte, peu important la date des faits ayant donné lieu au licenciement.
Elle fait ainsi primer la liberté d'expression sur toute autre considération et rappelle donc que toute sanction prise en violation de cette liberté fondamentale doit être frappée de nullité.
La Cour de cassation entend d'ailleurs donner une résonance toute particulière à cet arrêt qu'elle publiera au sein de son rapport annuel.
Pour cause, le sujet des lanceurs d'alerte est plus que d'actualité puisque la loi Sapin 2 telle que modifiée par le Sénat qui l'a adoptée le 8 juillet dernier doit passer en commission mixte paritaire prochainement avant d'être votée définitivement.
Article original de Frédéric Chhum, Avocat.

Original de l'article mis en page : Lanceurs d'alerte : nullité du licenciement d'un salarié ayant dénoncé de bonne foi des faits susceptibles de recevoir une qualification pénale. Par Frédéric Chhum, Avocat.

Seriez vous d’accord pour que WhatsApp partage vos données avec Facebook ?

Seriez vous d’accord pour que WhatsApp partage vos données avec Facebook ?

Les nouvelles règles de confidentialité de WhatsApp ne vont peut-être pas vous plaire.
Lorsque WhatsApp a annoncé son acquisition par Facebook en 2014, les utilisateurs et les défenseurs de la vie privée se sont inquiétés de ce qui allait advenir de leurs données. Pendant deux ans, les deux services sont restés indépendants. Cependant, aujourd'hui, WhatsApp a mis à jour ses règles de confidentialité, qui sont restées inchangées pendant 4 ans.
Et celles-ci n'excluent plus l'utilisation par Facebook des données du milliard de personnes utilisent WhatsApp pour optimiser ses publicités.

« […] en connectant votre numéro de téléphone avec les systèmes de Facebook, ce dernier peut vous offrir de meilleures suggestions d'amis et vous montrer des publicités plus pertinentes si vous avez un compte Facebook. Par exemple, vous pouvez voir une publicité d'une entreprise avec laquelle vous avez déjà travaillé au lieu de voir celle d'une entreprise dont vous n'avez jamais entendu parler », lit-on dans un communiqué de WhatsApp.

Cependant, le service explique aussi que cette « coordination » avec Facebook permettra également à WhatsApp de faire des choses comme « suivre des mesures de base sur la fréquence d'utilisation de nos services des gens et améliorer la lutte contre les spams ».

Et WhatsApp a bien clarifié que même si il va d'avantage collaborer avec Facebook, ses messages sont chiffrés de bout en bout, ce qui signifie que théoriquement, personne (ni Facebook, ni WhatsApp) ne peut accéder au contenu.

Le modèle économique de WhatsApp se précise

Pour rappel, WhatsApp était à l'origine une application payante, mais gratuite la première année. Cependant, le service a récemment décidé supprimer les frais annuels, pour devenir entièrement gratuit. Cependant, WhatsApp n'entend pas gagner de l'argent en affichant des bannières publicitaires, mais plutôt en misant sur des fonctionnalités pensées pour les relations entre clients et entreprises. Et les nouvelles règles de confidentialités reflètent aussi ce projet.
Article original de Setra

Réagissez à cet article

Original de l'article mis en page : WhatsApp va partager vos données avec Facebook