L’exploitant professionnel d’un hotspot Wi-Fi n’est pas responsable des contrefaçons

	L’exploitant professionnel d’un hotspot Wi-Fi n’est pas responsable des contrefaçons

Cour de justice de l'Union européenne a jugé aujourd'hui qu'un fournisseur de hotspot n'était pas responsable des contrefaçons réalisées par ses utilisateurs. Cependant, cet acteur pouvait se voir enjoindre d'exiger un mot de passe par une juridiction ou une autorité administrative nationale.

Le litige est né en 2010 : Sony Music avait adressé une mise en demeure à Thomas Mc Fadden. Cet exploitant d'une entreprise de sonorisation outre-Rhin avait laissé son réseau Wi-Fi ouvert sans mot de passe. Or, un tiers a pu mettre à disposition une œuvre du catalogue de la major. L'affaire était remontée jusqu'à la CJUE où les juridictions allemandes ont déversé une série de questions préjudicielles.

FAI ou exploitant de hotspot Wi-Fi, même combat

Dans son arrêt (PDF) du jour, la Cour va d'abord considérer que la fourniture d'un tel accès Wi-Fi relève de la fourniture d'un service de la société de l'information, à l'instar donc des prestations d'un FAI (article 12 de la directive de 2000). Cela implique cependant que l'exploitant du hotspot ait un rôle « *purement technique, automatique et passif* » et qu'il n'a ni la connaissance ni le contrôle des informations transmises.

Ceci vérifié, la Cour rappelle qu'un tel prestataire n'est alors pas responsable des contenus qui passent dans ses tuyaux à la triple condition :

1. de ne pas être à l'origine d'une telle transmission,
2. de ne pas sélectionner le destinataire de cette transmission et
3. de ne ni sélectionner ni modifier les informations faisant l'objet de ladite transmission.

Si ces conditions sont remplies, alors un titulaire de droit ne peut demander la moindre indemnisation à cet intermédiaire ou le remboursement de ses frais…[lire la suite]

Qu'en est-il des professionnels de l'hôtellerie qui mettent à disposition de leurs clients du Wifi ? Réagissez

---

Réagissez à cet article

Original de l'article mis en page : CJUE : l'exploitant professionnel d'un hotspot Wi-Fi n'est pas responsable des contrefaçons

Alerte : Une faille permet aux hackers de contrôler les connexions internet des particuliers

	Alerte : Une faille permet aux hackers de contrôler les connexions internet des particuliers

Les chercheurs F-Secure viennent de mettre à jour une faille critique présente sur certains des routeurs Inteno. Cette vulnérabilité est assez importante pour permettre à un pirate de prendre le contrôle total de l'appareil de la victime et des communications internet. Cette découverte met en lumière les problématiques de sécurité propres aux routeurs.

La vulnérabilité récemment détectée permet au pirate d'installer son propre firmware sur l'appareil, qui continuera, en apparence, à fonctionner comme avant…mais en coulisses, des backdoors et autres fonctionnalités pirates feront leur apparition. Le hacker sera capable de lire tout le trafic non-chiffré passant par le routeur : non seulement les communications appareil-internet, mais aussi celles établies entre deux appareils. Il pourra également manipuler le navigateur de la victime afin de la rediriger vers des sites malveillants.

« En remplaçant le firmware, le pirate peut changer n'importe quelle règle du routeur », explique Janne Kauhanen, Cyber Security Expert chez F-Secure. « Vous regardez du contenu vidéo stocké sur un autre ordinateur ? Alors, le pirate y a lui aussi accès. Vous mettez un jour un autre appareil à partir du routeur ? Pourvu que l'appareil en question ne renferme pas d'importantes vulnérabilités, sinon le pirate pourra également s'en saisir. Bien entendu, le trafic https est chiffré. Les pirates n'y auront pas accès facilement. Ils peuvent néanmoins vous rediriger systématiquement vers des sites malveillants afin d'installer des malware sur votre machine. »

« Le type de routeur en question reçoit des mises à jour firmware depuis un serveur associé au fournisseur d'accès de l'utilisateur. Problème : les routeurs vulnérables ne vérifient pas si la mise à jour est valide, ni si elle vient de la bonne source. Un pirate qui a déjà eu accès au trafic circulant entre le routeur et le serveur de mise à jour du FAI (par exemple, en accédant à la distribution réseau de l'immeuble où se trouve l'appartement) peut installer son propre serveur de mises à jour. Il peut ensuite installer son firmware malveillant.

Les chercheurs expliquent qu'il ne s'agit que de la partie émergée de l'iceberg en matière de sécurité routeurs. Les ordinateurs sont de mieux en mieux protégés mais les utilisateurs ignorent souvent que le routeur peut être lui aussi vulnérable.

« C'en est ridicule de constater à quel point les routeurs vendus sont peu sécurisés », explique Janne Kauhanen. « Nous trouvons des vulnérabilités routeurs en permanence. Les firmware utilisés par les routeurs et les objets connectés sont mal conçus. L'aspect sécurité est négligé tant par les fabricants que par les clients. Personne n'y porte attention, si ce n'est le pirate, qui utilise les vulnérabilités pour détourner le trafic internet, voler des informations, répandre des malware. »

La vulnérabilité détectée, bien que sévère, n'est pas immédiatement exploitable. Un pirate doit avoir déjà acquis une certaine position sur le réseau, en réalisant une incursion entre le routeur et le point d'entrée internet. Les routeurs concernés sur les Inteno EG500, FG101, DG201. D'autres modèles sont probablement concernés….[lire la suite]

Réagissez à cet article

Original de l’article mis en page : F-Secure : Une nouvelle faille, permettant aux hackers de contrôler les connexions internet des particuliers, révélée sur plusieurs routeurs – Global Security Mag Online

---

Les données d’une banque en partie détruites à la suite d’un test…

Les données d’une banque en partie détruites à la suite d’un test…

Le fonctionnement d'un datacenter à Bucarest en Roumanie a été complètement stoppé pendant plus de 10 heures suite à un phénomène rarissime.

Une banque roumaine a fait face à un arrêt complet de ses systèmes de paiement ainsi que de ses distributeurs automatiques pendant environ 10 heures suite à un dysfonctionnement de son système d'alarme anti-incendie. L'événement est particulièrement rare et inhabituel : le son a été produit par la diffusion d'un gaz inerte au cours d'un test routinier du système d'alarme incendie.

Non seulement celui-ci a forcé le datacenter à passer hors ligne, mais il a également causé la destruction d'une douzaine de disques durs, ce qui a provoqué de sérieux dommages.
La semaine dernière, Daniel Llano, directeur de la banque ING a expliqué à ses clients que les dysfonctionnements avaient été causés par une propagation de gaz Inergen.
L'Inergen est utilisé pour éteindre des incendies sans avoir besoin de passer par un liquide ou de la mousse, les méthodes plus traditionnelles. Utile dans les espaces clos, le gaz Inergen est conservé sous forme compressé dans des cylindres et celui-ci est dispersé via le système de canalisation pour empêcher la propagation d'incendies.
En temps normal, cette technique est idéale pour les datacenters. Les liquides ou la mousse pourraient en effet facilement endommager les équipements les plus sensibles. Mais dans ce cas précis, quelque chose est allé de travers.
Lorsque le gaz a été propulsé dans le système de ventilation, la pression de celui-ci était bien trop forte, ce qui a produit un son incroyablement fort lors de la libération du gaz Inergen.
Un porte-parole d'ING a expliqué à nos confrères de Motherboard que « l'exercice s'est déroulé comme prévu, mais nous devons faire face à des dommages collatéraux. »
Une autre source citée par la publication précise que le son produit par le système s'est révélé bien plus fort qu'escompté. Évalué à plus de 130Db, celui-ci a largement dépassé l'échelle des outils de mesure du son mis en place par la banque. Malheureusement, le son provoque des vibrations, qui se sont propagées aux boîtiers des disques durs et ont endommagé les composants internes.
Motherboard relate que la situation pouvait être comparée au fait « de placer une baie de stockage à côté d'un moteur d'avion à réaction. »…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Comment un simple son a mis un datacenter à genoux – ZDNet

Comment créer une copie d’écran la moins contestable possible ?

	Comment créer une copie d’écran la moins contestable possible ?

La copie d'écran sert souvent d'élément de preuve dans un dossier. Pourtant, sa réalisation demande de prendre un certain nombre de précautions pour éviter qu'elle ne soit contestée (et contestable).

Il m'est arrivé, au début de mon activité d'expert judiciaire en informatique, d'assister des huissiers de justice lors de la constitution de preuves, en matière de publication sur internet.
En clair, il s'agissait souvent d'aider un huissier à faire des copies d'écran.
Puis, avec le temps, les compétences informatiques des huissiers ont fortement augmenté, et il devient rare que l'on me demande de l'aide pour faire une copie d'écran.
Pourtant…
Parfois une copie d'écran peut être refusée par un tribunal, si elle ne présente pas un caractère probant suffisant. Extrait d'un jugement :
« Attendu que si la preuve d'un fait juridique n'est, en principe, et ainsi qu'en dispose l'article 1348 du Code civil, soumise à aucune condition de forme, il demeure néanmoins que lorsqu'il s'agit d'établir la réalité d'une publication sur le réseau internet, la production d'une simple impression sur papier est insuffisante pour établir la réalité de la publication, tant dans son contenu, que dans sa date et dans son caractère public, dès lors que ces faits font l'objet d'une contestation ; qu'en effet, et comme le souligne le défendeur l'impression peut avoir été modifiée ou être issue de la mémoire cache de l'ordinateur utilisé dont il n'est pas justifié que cette mémoire ait été, en l'occurrence, préalablement vidée ; »
Je propose pour ma part une méthode de copie d'écran d'une page web qui me semble respecter les règles de l'art :
Étape 1 : Choisir un ordinateur « sûr » pour établir le constat.
Étape 2 : Vider le cache local.
Étape 3 : Vérifier les DNS.
Étape 4 : Afficher la page incriminée.
Étape 5 : Imprimer la page.
Étape 6 : Recommencer avec un autre navigateur.
Étape 7 : Recommencer avec un autre ordinateur et un autre réseau.
[Plus de détails ?]

Réagissez à cet article

Original de l'article mis en page : Contestation d'une copie d'écran. Par Olivier Nerrand, Expert judiciaire.

Protection des données personnelles, plus que quelques mois pour se mettre en règle…

	Protection des données personnelles, plus que quelques mois pour se mettre en règle…

Il y a urgence à se former aux nouvelles obligations en matière de protection des données… Après 4 années de négociations très médiatisées, le nouveau règlement européen de protection des données a été adopté en mai 2016. Il sera applicable en France le 25 mai 2018. Mais une bonne moitié des organisations françaises ne sont toujours pas informées du contenu de la réforme concernant la protection des données.

Pourtant, il y a de vraies conséquences en termes de responsabilités et de sanctions ! En cas de violation des dispositions du règlement, les pénalités peuvent atteindre un montant maximal de 4% du CA mondial d'un groupe ou de 20 Millions d'euros.

De plus, tout organisme public ou privé victime d'un piratage, d'une faille de sécurité ou de tout acte risquant de compromettre ou ayant compromis la sécurité (confidentialité, intégrité) de données personnelles aura 72 heures pour signaler l'incident à la CNIL.
L'organisme devra, dans la plupart des cas informer les victimes (comme Orange a été obligé de le faire à deux reprise en 2014).
Pas bon pour l'image ça !
Imaginez, des années pour construire votre réputation et en quelques heures :
1. Vous devez signaler à la CNIL que vous vous êtes fais pirater et que des données personnelles ont été compromises ;
2. Vous allez très probablement avoir droit à un contrôle de la CNIL qui va venir rechercher la cause de cette faille et par la même occasion faire le point sur votre mise en conformité ;
3. Pour couronner le tout (le 3ème effet Kiss Cool), vous risquez d'informer vos clients, salariés, fournisseurs que leurs données personnes ont été piratées sur votre système informatique. Imaginez leur réaction !!! Toujours pas bon pour l'image ça !

La première étape pour se mettre en conformité est de s'informer et de sensibiliser le personnel qui a un rôle important à jouer dans cette mise sur rail.
Ensuite, il sera nécessaire de former une personne en particulier dans votre établissement. Actuellement il s'appellera CIL (Correspondant Informatique et Libertés), demain DPO (Délégué à la Protection des Données), cette personne va jouer un rôle clé dans votre mise en conformoté.
Il devra :
1. Contrôler le respect du règlement ;
2. Informer et conseiller le responsable du traitement (ou le sous-traitant en charge de cette mission) et les employés qui procèdent au traitement des données sur les obligations qui leur incombent.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** 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

---

Réagissez à cet article

Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie

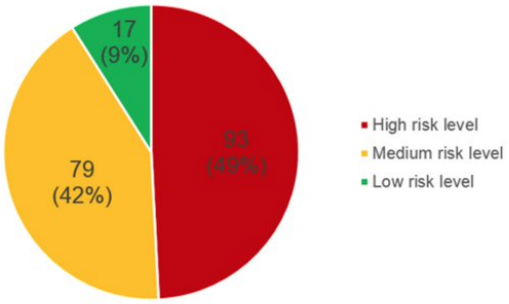
	Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie

On ne cesse de vous le répéter, il est très important de rester au courant des dernières actualités concernant la cybersécurité et ses menaces. Mieux vaut prévenir que guérir.

Cependant, même ceux qui connaissent tout en matière de cybersécurité, qui utilisent des mots de passe fiables et qui les changent régulièrement, qui reconnaissent des messages d'hameçonnage au premier coup d'œil et qui protègent leurs dispositifs avec une excellente solution de sécurité, même ceux qui font *tout*, ne sont pas totalement à l'abri. Tout simplement parce que nous vivons en société.

Le problème est que nous avons le contrôle sur nos objets personnels, mais pas sur celui des équipements industriels, qui est loin de notre portée.

Vous avez dit cybersécurité ?
Nos experts en cybersécurité ont mené une étude afin de découvrir où nous en sommes concernant la sécurité des systèmes de contrôle industriel.
Shodan, le moteur de recherche pour les dispositifs connectés, nous a montré que 188 019 systèmes industriels dans 170 pays sont accessibles sur Internet. La majorité d'entre eux sont localisés aux Etats-Unis (30,5%) et en Europe, essentiellement en Allemagne (13,9%), Espagne (5,9%) et en France (5,6%).



ICS vulnerabilities in 2015 by risk level (CVSS v.2 and CVSS v.3)

92% (172 982) des systèmes de contrôle industriel (SCI) détectés sont vulnérables. Lamentablement, 87% ont un niveau de risque moyen de bugs et 7% connaissent des problèmes critiques.
Ces cinq dernières années, les experts ont méticuleusement examiné de tels systèmes et y ont découvert de nombreuses failles de sécurité. Durant ce laps de temps, le nombre de vulnérabilités dans les composants SCI a multiplié par dix.
Parmi les systèmes que nos experts ont analysés, 91,6% ont utilisé des protocoles non sécurisés, en donnant l'opportunité aux cybercriminels d'intercepter ou de modifier les données utilisant des attaques de l'homme du milieu.
Egalement, 7,2% (environ 13 700) des systèmes appartiennent à de grandes compagnies aéronautiques, des transports et de l'énergie, pétrolières et gazières, métallurgiques, de l'industrie alimentaire, de la construction et autres secteurs primordiaux.

En d'autres termes, des hackers qualifiés peuvent influencer n'importe quel secteur économique. Leurs victimes (les entreprises piratées) porteraient préjudice à des milliers ou millions de personnes en leur fournissant de l'eau contaminée ou de la nourriture immangeable, ou en leur coupant le chauffage en plein hiver.

Qu'est-ce que cela implique pour nous tous ?

…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** 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

---

Réagissez à cet article

Original de l’article mis en page : Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Une garantie d’un million de dollars contre les ransomwares

Une garantie d’un million de dollars contre les ransomwares

Un éditeur de logiciels de cybersécurité propose de reverser jusqu'à un million de dollars à ses clients qui seraient, malgré ses protections, victimes d'un virus informatique.

Ce n'est pas une incitation à payer les rançonneurs informatiques. Hier, l'éditeur de logiciels de cybersécurité SentinelOne a annoncé proposer à ses clients professionnels une garanti d'un montant maximum d'un million de dollars contre toute menace qui percerait ses défenses. Notamment les ransomwares, ses programmes malveillants qui coupent l'accès aux données stockées dans les ordinateurs touchés et invitent à payer pour les récupérer. La police conseille de ne jamais céder à ce chantage.
SentinelOne compte sur sa technologie de machine learning pour protéger ses clients. En cas de manquement à ses devoirs, l'éditeur dédommagerait les entreprises à hauteur de 1.000 dollars par postes de travail et dans la limite d'un million de dollars. « *Avec cette assurance financière, nous devenons vraiment responsables de la sécurité de nos clients*, souligne Scott Gainey, le patron du marketing de SentinelOne,*jusqu'ici, les entreprises victimes qui voulaient se retourner contre leurs éditeurs d'anti-virus ne pouvaient pas, c'est injuste*. » D'après lui, cette garantie est une première au monde…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** 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

---

Réagissez à cet article

Original de l'article mis en page : Une garantie d'un million de dollars contre les ransomwares, Cybersécurité — Les Echos Business

---

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