Drone piégé utilisé par l’EI contre deux militaires français

Drone piégé utilisé par l’EI contre deux militaires français

Selon des informations du Monde, deux militaires français qui étaient en opération auprès des Kurdes en Irak ont été rapatriés en France après avoir été grièvement blessé par un drone piégé de l'État islamique.

C'est un mode d'action que les forces de l'ordre redoutent sur le territoire national, et qui semble désormais déployé sur le terrain de l'adversaire. Le Monde affirme ce mardi que deux militaires français ont été gravement blessés par un drone qui avait été piégé par des militants de l'État islamique, en Irak. L'un des deux serait entre la vie et la mort.
« Les deux commandos ont été touchés par un drone volant piégé, envoyé par un groupe lié à l'EI, dans des circonstances qui restent à préciser. Les militaires auraient intercepté le drone, avant que celui-ci explose à terre. Ce mode d'action contre des forces françaises est en tout état de cause inédit », rapporte le quotidien, qui précise que ses informations sont confirmées par d'autres médias.
Ce piège aurait été tendu aux commandos parachutistes qui intervenaient auprès des forces kurdes à Erbil, dans le nord de l'Irak, entre Mossoul et Kirkouk. La ville est la capitale de la région autonome du Kurdistan.

Le Monde indique que le ministère de la Défense ne souhaite pas confirmer cette attaque d'un nouveau genre et le rapatriement des deux soldats à l'hôpital militaire de Percy-Clamart, non seulement par souci de protéger les familles, mais aussi peut-être en raison des « moyens employés pour cette attaque » (on peut ajouter que de manière plus générale s'agissant des propagandes de guerre, les armées n'aiment jamais communiquer sur leurs propres pertes, préférant mettre en avant leurs réussites pour conserver le moral des troupes et le soutien des populations).

LA CRAINTE D'UN ATTENTAT PAR DRONE

La crainte est sans doute que le mode opératoire, relativement peu coûteux et surtout peu risqué pour les attaquants, ne donne des idées sur le front irakien ou syrien, mais aussi en occident. L'hypothèse qu'une petite bombe puisse être transportée par un drone sans savoir d'où il a décollé et d'où il est contrôlé est soulevée depuis longtemps par les experts de la sécurité aérienne. Elle avait notamment été évoquée en France lors du survol des centrales nucléaires par des drones.
Depuis, le législateur s'est emparé du sujet en élaborant une proposition de régulation des drones en cours d'examen, qui prévoit notamment l'obligation d'identifier les drones à distance ou de brider leur utilisation dans certaines zones réglementées. Mais par définition les lois n'ont aucune influence contre ceux qui veulent les violer, et il paraît bien difficile d'empêcher totalement le transport de bombes par drone, sauf à utiliser des moyens technologiques encore balbutiants et impossibles à déployer sur tout le territoire comme des brouilleurs, des lasers, des perturbateurs de signaux GPS, des filets, ou même des aigles.

UNE RÉPONSE ARTISANALE À L'UTILISATION DE « ROBOTS TUEURS » ?

Le fait que les troupes de l'EI utilisent des bombes montées sur des drones n'est aussi, hélas, qu'une réponse attendue à l'utilisation croissante des drones et autres engins militaires conduits à distance par les troupes alliées. En août dernier, l'armée irakienne était fière de présenter un fusil mitrailleur monté sur un véhicule conduit à 1 km de distance, qui permettait d'aller tuer sans risquer de se faire tuer, ce qui est aussi l'objectif des avions de combat semi-autonomes, des navires de guerre ou des nouveaux chars d'assaut. L'utilisation de drones piégés n'est à cet égard qu'une réponse artisanale de même nature.
Il faut ajouter qu'en droit international, l'utilisation de telles armes n'est pas interdite dès lors qu'elles visent à tuer des militaires combattants, et non des civils. La question de la régulation des « robots tueurs » a déjà fait l'objet de débats dans la communauté internationale, dans le cadre de révisions des conventions de Genève, mais les perspectives d'un accord sont excessivement lointaines. La seule piste évoquée, encore très incertaine, est l'obligation qui pourrait être faite qu'un humain reste en permanence aux commandes des engins robotisés, pour ne pas parvenir à des guerres menées par IA interposées.
[Article source]

Réagissez à cet article

Original de l'article mis en page : L'État islamique aurait piégé un drone et blessé grièvement deux militaires français — Politique — Numerama

---

Les 15 mesures clés de la loi Numérique

Les 15 mesures clés de la loi Numérique

Vous n’avez guère suivi les débats autour du projet de loi Numérique, qui vient tout juste d’être définitivement adopté par le Parlement ? Voici un panorama de quinze mesures emblématiques. Élan en faveur de l’Open Data.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l’étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s’en protéger** (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d’informations sur sur cette page.

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

Le projet de loi République Numérique enfin adopté

Le projet de loi République Numérique enfin adopté

Après avoir été adopté par l'Assemblée Nationale au mois de juillet dernier, le projet de loi République Numérique l'a été à son tour par le Sénat. Sauf saisine du Conseil Constitutionnel dans les 15 prochains jours, la loi devrait donc être promulguée rapidement et plusieurs choses devraient donc changer dans les semaines à venir.

L'open data, une des nouveautés du projet de loi République Numérique

A l'occasion de sa séance publique du 28 septembre 2016, le Sénat a adopté définitivement le projet de loi « République Numérique » et ce à l'unanimité.
Deux mois après, les sénateurs font donc le même choix que les députés ce qui signifie que la promulgation de ce texte est pour bientôt.
Parmi les nouveautés qu'il apporte, il y a l'open data. En effet, ce projet de loi prévoit l'ouverture d'une partie des données de l'administration publique mais aussi des données de certaines sociétés du secteur privé ayant une mission de service public. Ceci est en particulier une grande avancée pour la recherche puisque des données à l'accès restreint seront accessibles à un public plus large.

Vers un meilleur accès aux réseaux numériques

Initié par Axelle Lemaire, secrétaire d'Etat chargée du Numérique, le projet de loi République Numérique a vocation à faciliter l'entrée de la République dans l'ère du numérique.
Par conséquent, les idées et mesures présentes dans le texte sont nombreuses et variées et visent à :

- Améliorer la protection des données sur le web
- Rendre accessible Internet au plus grand nombre
- Mettre en concurrence tous les acteurs de l'Internet
- Rendre obligatoire l'information « claire et loyale » des clients
- Accélérer la couverture du territoire en très haut débit
- Rendre accessible les contenus numériques aux personnes souffrant de handicap (visuel, auditif, etc…)
- Reconnaître le e-sport et définir le statut des joueurs

Autrement dit, la loi République Numérique devrait éclaircir bien des situations et cas complexes…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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 : Le projet de loi République Numérique enfin adopté

Professionnels, ne pas fermer votre Wi-Fi pourrait vous coûter cher

Professionnels, ne pas fermer votre Wi-Fi pourrait vous coûter cher

En jugeant que les titulaires de droits d'auteur pouvaient exiger des professionnels qu'ils recueillent l'identité de quiconque utiliserait leur réseau Wi-Fi, la CJUE a prévenu qu'ils pourraient se faire rembourser l'intégralité des frais de justice engagés.

Jeudi, nous rapportions qu'avec sa décision *Tobias Mc Fadden* prise pour une affaire de piratage de fichiers MP3, la Cour de justice de l'Union européenne (CJUE) a véritablement condamné à mort les réseaux Wi-Fi ouverts, en exigeant que les professionnels qui offrent un tel service recueillent l'identité des internautes qui s'y connectent, et conservent un journal de leurs connexions. Ceux qui ne le font pas s'exposeront à des conséquences financières, alors-même que la Cour estime qu'ils ne sont pas responsables des téléchargements illégaux effectués avec leur connexion.

Pour comprendre ce paradoxe apparent, il faut revenir sur le raisonnement juridique de la CJUE.
Tout d'abord, les juges reconnaissent que le professionnel qui met à disposition de ses clients ou prospects un réseau Wi-Fi est assimilable à un « fournisseur d'accès à un réseau de communication », autrement dit à un FAI. En conséquence, ils déduisent que la jurisprudence de la Cour qui interdit d'imposer le filtrage à un FAI s'applique, et que le fournisseur du Wi-Fi ne peut pas être tenu pour responsable de l'utilisation qui est faite par les utilisateurs.
Dès lors, « *il est en toute hypothèse exclu que le titulaire d'un droit d'auteur puisse demander à ce prestataire de services une indemnisation au motif que la connexion à ce réseau a été utilisée par des tiers pour violer ses droits* », juge la Cour…[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

---

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 : Professionnels, ne pas fermer votre Wi-Fi pourrait vous coûter cher – Politique – Numerama

---

Peut-on être condamné pour avoir visité des sites djihadistes ?

Peut-on être condamné pour avoir visité des sites djihadistes ?

Un jeune homme de 28 ans, qui était surveillé par les services de renseignement pour des velléités de départ vers la Syrie, a été condamné à deux ans de prison par le tribunal correctionnel de Marseille, pour avoir régulièrement visité des sites djihadistes à la bibliothèque municipale.

Jeudi, le tribunal correctionnel de Marseille a condamné un Marseillais de 28 ans à deux ans de prison, parce qu'il avait consulté à de nombreuses reprises des sites de propagande terroriste, et notamment regardé des scènes d'exécutions.
La justice a fait une pleine application des nouvelles dispositions du code pénal introduites par la loi Urvoas du 3 juin 2016, qui punissent d'un maximum de deux ans de prison « *le fait de consulter habituellement un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie* ».
Seule la démonstration de la bonne foi de l'internaute pouvait l'exonérer d'une condamnation. Mais en l'espèce, et même s'il a tenté de plaider qu'il faisait un travail d' « apprenti journaliste » avec un « programme de recherches », les éléments contextuels rapportés par l'AFP permettaient difficilement de croire à une simple volonté de s'informer :
De janvier à août, il s'était connecté à 143 reprises pour visionner écrits et vidéo faisant l'apologie du terrorisme. Il a été interpellé le 9 août alors qu'il faisait des recherches sur le moyen de gagner la Libye via l'Espagne. Jugé en comparution immédiate, il avait été placé en détention dans l'attente de son procès. Hospitalisé en 2012 en psychiatrie à Avignon où il dit s'être converti à l'islam, le jeune homme était surveillé par les services du renseignement depuis l'été 2015, date à laquelle son père avait alerté les autorités sur les velléités de départ en Syrie de son fils.
Ce signalement avait provoqué une interdiction administrative de quitter le territoire pour six mois. Son téléphone portable contenait plus de 100 vidéos dont l'une de 21 minutes montrant la décapitation de quatre hommes.
Ce n'est pas la première condamnation du genre depuis que le législateur a fait de la seule consultation des sites terroristes une infraction pénale en elle-même (auparavant, il fallait que d'autres éléments matériels viennent en soutien). Mais cette affaire est intéressante à un autre titre…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Un homme condamné pour avoir visité des sites djihadistes à la bibliothèque – Politique – Numerama

---

Extension de règles de sécurité des opérateurs aux acteurs du Net en Europe

Extension de règles de sécurité des opérateurs aux acteurs du Net en Europe

---

En proposant de nouvelles règles télécom cette semaine, la Commission européenne introduirait des obligations de sécurité aux services de messagerie. Des obligations déjà en vigueur pour les opérateurs, qui réclament une parité réglementaire avec les acteurs en ligne.

Équilibrer les obligations entre opérateurs et messageries en ligne ressemble souvent à un travail de funambule, dans lequel se lancerait la Commission européenne. Dans quelques jours, l'institution doit dévoiler une révision des règles télécoms en Europe. Selon un brouillon obtenu par Reuters, elle y introduirait des obligations de sécurité pour les services de messagerie en ligne, déjà appliquées par les opérateurs.

Des obligations de signalement des brèches

À la mi-août, plusieurs médias affirmaient que la Commission européenne comptait proposer cette parité entre acteurs. Le brouillon obtenu par Reuters viendrait donc confirmer cette piste. Dans celui-ci, les services « over the top » devront ainsi signaler les brèches « *qui ont un impact important sur leur activité* » aux autorités et disposer d'un plan de continuité de l'activité. Les services qui proposent des numéros de téléphone ou d'en appeler, comme Skype, devront aussi permettre les appels d'urgence.

Pourtant, ces règles pourront être plus légères pour ces services que pour les opérateurs classiques, dans la mesure où les services ne maîtrisent pas complètement la transmission des contenus via les tuyaux. Dans l'absolu, ces règles doivent réduire l'écart d'obligations entre les acteurs télécoms et ceux d'Internet, avec en toile de fond le combat entre des acteurs européens et des sociétés principalement américaines.

Rappelons que le règlement sur les données personnelles, voté en avril par le Parlement européen, doit lui aussi obliger les services à divulguer aux autorités les fuites de données, dans un délai court. En France, cette obligation ne concerne que les opérateurs.

Le moment est d'ailleurs pour celle-ci, le secteur télécom étant notamment le théâtre de lobbyings intenses. Elle a d'ailleursretiré une proposition de « fair use » pour la fin des frais d'itinérance il y a quelques jours, suite à des levées de bouclier du côté des associations de consommateurs, des opérateurs et des eurodéputés. Comme le rappelle Reuters, ce texte passera entre les mains du Parlement et du Conseil de l'Europe, avec des changements possibles à la clé…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : L’UE préparerait l’extension de règles de sécurité des opérateurs aux acteurs du Net

---

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 ?]

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

---

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 : Contestation d’une copie d’écran. Par Olivier Nerrand, Expert judiciaire.

CNIL : nouvelle norme simplifiée pour la scolarité des mineurs

	CNIL : nouvelle norme simplifiée pour la scolarité des mineurs

---

Dans le cadre de son programme de simplification des formalités préalables pour les collectivités territoriales, la Cnil a adopté une norme simplifiée unique qui met à jour et abroge le cadre existant.

Le 10 décembre 2015, la Commission a adopté une norme simplifiée n°NS-058 qui fusionne et abroge les normes simplifiées n°NS-027 et n°NS-033. En effet, ces normes étaient désuètes et ne répondaient pas aux nouvelles préoccupations des acteurs concernés. Elle a été présentée sur le site de la Cnil le 12 août dernier.
Cette nouvelle norme permet de simplifier, pour ces traitements courants, les démarches des collectivités territoriales et des organismes en charge d'un service scolaire, périscolaire et de petite enfance. Elle offre un cadre unifié et adapté aux contraintes liée à la gestion de ces services.
Après avoir vérifié que leur traitement s'inscrit précisément dans le champ d'application de cette norme, les responsables de traitements de données concernés devront effectuer un engagement de conformité à la norme NS-058 auprès de la CNIL.

Les personnes concernées

Cette norme s'adresse aux collectivités territoriales, aux personnes morales de droit public et aux personnes morales de droit privé gérant un service public…[lire la suite]

En savoir plus

Le communiqué de la Cnil du 12 août dernier avec une présentation synthétique de la norme :
https://www.cnil.fr/fr/une-nouvelle-norme-simplifiee-ns-058-pour-la-gestion-des-affaires-scolaires-periscolaires
Le résumé succinct de la norme :
https://www.cnil.fr/fr/declaration/ns-058-affaires-scolaires-periscolaires-extrascolaires-et-petite-enfance
La norme NS-058 elle-même sur *Légifrance* :
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032788919

Réagissez à cet article

Original de l'article mis en page : Données personnelles : nouvelle norme simplifiée pour la scolarité des mineurs

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

---

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

Est-ce qu’un lien vers un contenu illégal est lui aussi illégal ?

Est-ce qu’un lien vers un contenu illégal est lui aussi illégal ?

Le fait de publier un lien renvoyant vers un contenu illicite est lui-même constitutif de contrefaçon ? À cette éminente question, la Cour de justice de l'Union européenne vient de répondre que non, sous deux importantes réserves : que le lien litigieux ait été diffusé sans but lucratif et que son auteur n'ait pas eu connaissance de son illicéité.

C'est suite à une saisine de la Cour de cassation des Pays-Bas que la justice européenne a rendu son arrêt de ce jour. Au cœur de ce dossier, un vrai jeu du chat et de la souris. Une dizaine de photos d'une présentatrice hollandaise furent hébergées sur FileFactory, puis « linkées » sur Geenstijl.nl, important site néerlandais. Le renvoi vers ces images, destinées à être publiées dans l'édition nationale de Playboy, avait rapidement provoqué la colère de la revue de charme. Sauf que même après avoir réussi à obtenir leur retrait de FileFactory, de nouveaux liens furent établis par Geenstijl.nl, cette fois via ImageShack.us notamment…
D'où la question : publier des liens vers ces images signalées comme manifestement illicites constituait-il un nouvel « acte de communication » d'une œuvre au public au sens de la directive européenne relative au droit d'auteur – dès lors soumis à l'autorisation obligatoire (et préalable) des ayants droit ? Pour la CJUE, la réponse est oui…[lire la suite]
L'arrêt de la CJUE (PDF)

Réagissez à cet article

Original de l'article mis en page : La CJUE juge qu'un lien

vers un contenu illégal peut être illégal