

RGPD Règlement européen sur la protection des données : Un cadre juridique unifié pour l'ensemble de l'UE

	<p>RGPD Règlement européen sur la protection des données : Un cadre juridique unifié pour l'ensemble de l'UE</p>
---	--

Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Le même texte s'appliquera donc dans toute l'Union. Le règlement est applicable à partir du 25 mai 2018. De plus, les traités déjà en vigueur à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.

Un champ d'application étendu
 Le critère de ciblage
 Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais *targeted*).
 En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.
 La responsabilité des sous-traitants
 Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitement », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.
 Les entreprises seront en contact avec un « **guy du stop shop** » : à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal », désigné comme l'autorité « chef de file ». Cet établissement sera soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités de traitement. Les entreprises bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettent en œuvre des traitements transnationaux.


Une coopération renforcée entre autorités pour les traitements transnationaux
 Identification des lieux où se trouvent des « établissements » – quel qu'il concerne les citoyens de différents États membres –. Les autorités de protection des données des différents États concernés seront juridiquement compétentes pour l'assurer de la conformité des traitements de données mis en œuvre.
 Afin d'assurer une réponse unique pour l'ensemble du territoire de l'Union, l'autorité « chef de file » coopère avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanction.
 Les autorités de protection nationales sont rattachées au sein d'un Comité européen de la protection des données (CEPD), qui veille à l'application uniforme du droit sur la protection des données. Il a vocation à remplacer l'Article 29.
 En pratique, l'autorité « chef de file » propose les mesures ou décisions (concernant le contenu d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD qui rend alors un avis. Ce avis est contraignant et doit être suivi par l'autorité « chef de file ».
 Dans le CEPD, mais si son avis n'est pas suivi, l'autorité « chef de file » partage la décision avec les homologues. Il y aura donc une décision conjointe, susceptible de recourir devant le juge des décisions de l'autorité « chef de file ».
 Par exemple, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL sera le guichet unique de cette entreprise et lui communiquera les décisions adoptées dans le cadre de sa mission de cohésion. Ses décisions seront ensuite, et elles sont définitives, susceptibles de recourir devant le Conseil d'État.
 Le mécanisme permet ainsi aux autorités de protection des données de se proposer rapidement sur la conformité d'un traitement ou sur un engagement au règlement et garantit une autorité juridique élevée aux entreprises en leur assurant une réponse unique sur l'ensemble du territoire de l'Union.

Besoin d'un accompagnement pour vous mettre en conformité avec le RGPD ?
 Besoin d'une formation pour apprendre à vous mettre en conformité avec le RGPD ?
 Contactez-nous

À lire aussi :
 Mise en conformité RGPD : Mode d'emploi
 Formation RGPD : L'essentiel sur le règlement européen pour la Protection des Données Personnelles
 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
 Règlement (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016
 Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
 Commentaire le Règlement Européen sur les données personnelles en 6 étapes
 Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des Données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
 Par des actions de formation, de sensibilisation ou d'aide dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement, l'habilitation de la Direction de Travail de l'Hôpital et de la Fonction Professionnelle « RB du DPO RD »
 Plus d'informations sur la Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Vous souhaitez en savoir plus sur nos services offerts en « Cloud » ?
 Contactez-nous sur contact@le-net-expert.fr



Le Net Expert
 INFORMATIQUE
 CONSULTING

Régistrez à cet article

Source : Règlement européen sur la protection des données : que faut-il savoir ? | Besoin d'aide | CNIL

Attention aux démarchages trompeurs « Mise en conformité RGPD »

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES LENETEXPERT.fr</p>	 <p>LE NET EXPERT MISES EN CONFORMITÉ</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>Denis JACOPINI EXPERT INFORMATIQUE ASSERMENTÉ SPÉCIALISÉ EN CYBERCRIMINALITÉ vous informe</p>		<p>Attention aux démarchages trompeurs « Mise en conformité RGPD »</p>			

Des courriers « Mise en conformité – RELANCE » ou « Mise en conformité – dernier rappel » avec le logo usurpé de la CNIL ou des fax « RGPD – Mise en conformité » invitent à appeler un numéro de téléphone pour ensuite facturer la fausse mise en conformité au règlement européen.



D'après des témoignages récents, après avoir appelé au numéro indiqué sur leur document affichant fièrement une bande bleu / blanc / rouge, ils ont posé quelques questions sur l'entreprise puis envoyé par mail un facture proforma demandant de s'en acquitter sous 72h. Les escrocs vont même jusqu'à dire qu'en payant cette facture, la CNIL fera une « levée de contrôle et de sanction » sur votre société. Puis, une fois le paiement effectué, vous aurez un entretien de 15 minutes durant lequel 50 questions vous seront posées puis sous 30 jours un « délégué syndical du département » prendra contact et clôturera définitivement la mise à jour. **Tous ces arguments sont strictement faux !**

La mise en conformité au RGPD nécessite plus qu'un simple échange ou l'envoi d'une documentation. Elle suppose un vrai accompagnement, par une personne qualifiée en protection des données personnelles, pour identifier les actions à mettre en place et assurer leur suivi dans le temps. Il est nécessaire, avant tout engagement, de chercher en ligne des informations sur la société qui prend contact avec vous. Si le doute persiste, vous pouvez contacter la CNIL au 01 53 73 22 22.

Pour vous rassurer, Denis JACOPINI et son équipe réalisent des démarches de mise en conformité des établissements avec la réglementation relative aux données à caractère Personnel depuis 2012. Plus d'informations ici

Nos conseils

Mettre en conformité nécessitera dans la plupart des cas une analyse de vos process, une sensibilisation du personnel, des interviews personnalisés et nous recommandons a minima une rencontre. Ces organismes ne semblent pas répondre à ces recommandations.

Au regard de pratiques commerciales trompeuses, la DGCCRF et la CNIL formulent plusieurs recommandations qui visent à :

- vérifier l'identité des entreprises démarcheurs qui ne sont en aucun cas, contrairement à ce que certaines prétendent, mandatées par les pouvoirs publics pour proposer à titre onéreux des prestations de mise en conformité au RGPD ;
- vérifier la nature des services proposés :
 - la mise en conformité au RGPD nécessite plus qu'un simple échange ou l'envoi d'une documentation. Elle suppose un vrai accompagnement par un professionnel qualifié en protection des données personnelles, pour identifier les actions à mettre en place et assurer leur suivi dans le temps ;
 - Dans certains cas, il peut aussi s'agir de manœuvres pour collecter des informations sur une société en vue d'une escroquerie ou d'une attaque informatique.

Principaux réflexes à avoir en cas de démarchage

Si vous recevez ce type de sollicitations, vous devez :

- demander des informations sur l'identité de l'entreprise démarcheuse permettant de faire des vérifications sur internet ou auprès des syndicats de votre profession ;
- demander le numéro SIRET de l'organisme ;
- demander les conditions générales de vente de l'organisme ou les termes du contrat que vous devrez signer ;
- consulter le site internet et vérifier les mentions légales ;
- vérifier l'ancienneté du nom de domaine (un nom de domaine récent indique la création récente du service avec un risque de manque d'expérience ou la création d'un nom de domaine spécialement pour l'arnaque.
- vous méfier de telles communications prenant les formes d'une information officielle émanant d'un service public ;
- lire attentivement les dispositions contractuelles ou pré-contractuelles ;
- prendre le temps de la réflexion et de l'analyse de l'offre ;
- diffuser ces conseils de vigilance auprès de vos services et des personnels qui sont appelés à traiter ce type de courrier dans l'entreprise ;
- ne payer aucune somme d'argent au motif qu'elle stopperait une éventuelle action contentieuse.

Pour vous aider dans votre mise en conformité au RGPD, la CNIL publie des contenus pratiques. Vous pouvez notamment consulter « RGPD : ce qui change pour les pros » ainsi que le nouveau « Guide de sensibilisation pour les petites et moyennes entreprises » élaboré en partenariat avec la BPI.

Pour information, voici les 6 phases recommandées par la CNIL

<https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes>

et notre méthode de mise en conformité avec le RGPD :

- « Comment se mettre en conformité avec le RGPD ? »
- « Mise en conformité RGPD : Accompagnement personnalisé par un Expert »
- « Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants ».



Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel), consultant depuis 1996 et formateur depuis 1998. J'ai bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, j'ai été ensuite Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur. **"Mon objectif est de mettre à disposition toute mon expérience pour mettre en conformité votre établissement avec le RGPD."**

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Vigilance : Démarchages trompeurs « Mise en conformité RGPD »* | CNIL

Illustration issue d'un témoignage

Votre responsabilité engagée en cas de piratage de vos données | Denis JACOPINI



**Votre
responsabilité
engagée en
cas de piratage de
vos données**

Si vous vous faites pirater votre ordinateur ou votre téléphone, votre responsabilité pourrait bien être engagée vis-à-vis des données que ce support numérique renferme.

Imaginez que vous disposez de différents appareils numériques informatiques renfermant une multitude de données, dont des données d'amis, de prospects, de clients, de fournisseurs (tout ce qu'il y a de plus normal), et tout à coup, à cause d'un malware (maliciel selon D. JACOPINI), un pirate informatique en prend possession de ces données, les utilise ou pire, les diffuse sur la toile. Que risquez-vous ?

En tant que particulier victime, pas grand chose, sauf s'il est prouvé que votre négligence est volontaire et l'intention de nuire retenue.

Par contre, en tant que professionnel, en plus d'être victime de piratage (intrusion causée par une faille, un virus, un cryptovirus, un bot, un spyware), et d'avoir à assumer les conséquences techniques d'un tel acte illicite pourtant pénalement sanctionné notamment au travers de la loi Goffrain du 5 janvier 1988 (première loi française réprimant les actes de criminalité informatique et de piratage), vous risquez bien de vous rendre une seconde cible vis-à-vis de la loi Informatique et Libertés du 6 janvier 1978 :

En effet, les entreprises, les sociétés, tous ceux exerçant une activité professionnelle réglementée ou non, les associations, les institutions, administrations et les collectivités, sont tenues de respecter la loi Informatique et Libertés du 6 janvier 1978 et notamment la sécurité des données selon les termes de son Article n°34 :

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

De plus, les sanctions jusqu'alors limitées à 5 ans d'emprisonnement et 300 000 euros d'amendes vont à partir du 25 mai 2018, par la mise en application du RGPD (Règlement Général sur la Protection des Données) être portées à 20 millions d'euros et 4% du chiffre d'affaire mondial.

Partons d'un cas concret.

La société Cochabonardais voit son système informatique piraté. Des investigations sont menées et le pirate informatique arrêté.

Vis-à-vis de la loi Goffrain du 5 janvier 1988, le voleur risque jusqu'à 2 ans de prison et 20 000 euros d'amende. Or ce voleur, après avoir découvert que la société Cochabonardais n'était pas en règle avec la CNIL la dénonce auprès de cette dernière.

Le responsable du traitement, généralement le chef d'entreprise risquera, lui, 5 ans de prison et 300 000 euros d'amende, une peine bien supérieure à son voleur.

Est-ce bien normal ?

Non, mais pourtant c'est comme ça et ça peut être le cas de toutes les entreprises, administrations et administrations françaises en cas de piratage de leurs ordinateurs, téléphones, boîtes e-mail.

Autre cas concret

Monsieur Roudbouou-Maitout voit son téléphone portable mal protégé et exposé aux virus et aux pirates. Un jour il apprend par un ami que les contacts de son téléphone se sont fait pirater. Il se déplace à la Police ou à la Gendarmerie, dépose une plainte mais le voleur n'est jamais retrouvé. Qui est responsable de cette fuite d'informations ?

La première chose à savoir, c'est si ce téléphone est professionnel ou personnel. S'il est professionnel, réfère vous au cas précédent. Si par contre le téléphone portable est personnel, vis-à-vis de la loi Informatique et Libertés, les particuliers ne sont pour l'instant pas concernés par l'obligation de sécurisation des données.

Ainsi, si la faute volontaire du propriétaire de l'appareil n'est pas retenue, le seul responsable de cette fuite de données sera et restera l'auteur du piratage.

Denis JACOPINI est Expert Informatique et aussi formateur en Protection des données personnelles (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 04 6204 04).

Nous pouvons vous assister des actions de sensibilisation en de formation à la Protection des Données Personnelles, au risque informatique, à l'hygiène informatique et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.le-net-expert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles>

Denis JACOPINI

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

- Expertises techniques (virus, spyware, phishing, malware, attaques DDoS, et autres menaces informatiques, réseaux sans fil, réseaux sociaux, sécurité des données...)
- Expertise de sécurité de vos dispositifs ;
- Formation et conférences en cybersécurité ;
- Responsable ICA (Commissariat Informatique et Internet) ;
- Accompagnement à la mise en conformité CNIL en entreprise ;

Le Net Expert
INFORMATIQUE
COURSILLOTTES

Réagissez à cet article
Original de l'article mis en page : [Informatique et Libertés : suis-je concerné ?](#) | CNIL

Les bons réflexes contre les attaques informatiques | Denis JACOPINI

✕

Les bons réflexes contre les attaques informatiques

350 milliards d'euros par an : selon le McAfee Report on the Global Cost of Cybercrime publié en 2014, tel est le coût estimé des attaques informatiques à l'échelle mondiale. Depuis le début de l'année, les attaques se sont multipliées, notamment suite aux attentats de Charlie Hebdo, mettant plus que jamais en péril la sécurité des données des entreprises et des institutions. Un rapport publié le 16 février dernier par Kaspersky Lab a quant à lui révélé l'attaque d'une centaine de banques depuis 2013 par un gang organisé.

Afin d'appréhender au mieux ces offensives, il est important d'en comprendre les tenants et les aboutissants et d'avoir à l'esprit les réflexes qui permettent de s'en prémunir.

Des attaques aux motivations multiples

De plus en plus de sites internet sont victimes d'attaques dites de « défiguration » perpétrées par des hacktivistes revendiquant des convictions religieuses, politiques ou encore contestataires. On trouve également certains attaquants qui agissent uniquement pour l'amusement, mais ces scénarios se font de plus en plus rares. En général, seule la page d'accueil du site est modifiée pour signifier leur passage et évoquer leurs revendications.

On trouve également d'autres attaques qui, elles, sont plus furtives (ou en tout cas tentent de l'être) et consistent à voler des informations à des fins de rançonnement par exemple. Les vols de données bancaires (carte de crédit, numéros de comptes) permettent quant à eux du détournement d'argent, l'achat de services ou encore de matériels en ligne. Ces criminels, bien organisés, offrent des services de tout type à d'autres criminels : du kit d'infection, à l'envoi de spam massif, en passant par des serveurs de contrôle (C&C) pilotant des milliers de machines « zombies » permettant des attaques DDoS (Déni de service distribué). Tous n'ont pas le même niveau technique, certains ne sont d'ailleurs que des « presse-bouton », alors que d'autres ont la capacité de créer des virus, ou des programmes exploitant des failles de sécurité.

Mais comment s'y prennent-ils ? Ces malfaiteurs utilisent une faille de sécurité dans un programme qui peut provenir d'une erreur de conception (un protocole mal sécurisé par exemple), de programmation ou d'implémentation (failles connues comme shellshock, heartbleed ou ghost), de configuration (oubli du mot de passe par défaut après une installation) ou encore d'une erreur d'utilisation par une personne utilisant un mot de passe trop faible par exemple. L'humain est donc au centre de cette problématique.

Le plus souvent ces attaques débouchent sur du détournement d'argent ou la diffusion de données sur internet. Les conséquences financières pour les entreprises peuvent être considérables, sans compter l'impact que cela peut avoir sur l'image de l'entreprise victime d'un piratage. Dès lors, quels réflexes adopter face à ces diverses attaques et failles ?

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

Contactez-nous

Adopter les bonnes pratiques pour limiter les risques

Les attaques ne cessent de croître dans la mesure où l'enjeu financier pour les criminels est très important. Lorsque l'on sait que l'attaque par déni de service est accessible pour seulement 30 à 70 dollars la journée et qu'un spam ne revient qu'à 10 dollars par tranche d'1 million d'e-mails*, ce type de pratique n'est pas prêt de cesser. A ce premier enjeu s'ajoute le manque de vigilance dont font preuve les internautes. Le risque de s'infecter est en effet omniprésent : il suffit de cliquer sur un lien drainant un logiciel malveillant ou encore de partager un contenu infecté.

Quand bien même le risque zéro n'existe pas, la grande majorité de ces attaques pourrait être bloquée, dès lors que l'on adopte les bonnes pratiques pour se protéger et protéger autrui. Le maître mot est l'anticipation et la capacité à réagir rapidement en cas d'intrusion, la mise en œuvre d'un pare-feu ou d'un anti-virus pour se protéger n'étant pas suffisante. Le processus organisationnel de sécurisation est en effet plus important que les outils de protection eux-mêmes (on a en général un rapport de 80-20).

Pour ce faire, l'un des points majeurs est la gestion des mises à jour. Lorsqu'une faille tombe, celle-ci peut-être déjà exploitée plus ou moins massivement. S'en suit la douloureuse phase consistant à tester si le programme régresse ou non dans son fonctionnement avant une mise en production. Durant toute cette période, le programme est encore exposé à une potentielle exploitation de la faille. Cela sous-entend qu'il faut d'une part valider aussi vite que possible, et d'autre part essayer de se protéger temporairement avec des outils de type Firewall ou IPS. Il est aussi bon de rappeler que ces outils de protection sont aussi faillibles que les autres et qu'ils peuvent être contournés.

Dans le cas où l'attaque a déjà eu lieu, sur un site web par exemple, la première chose à faire est de bloquer le site. Cette phase est primordiale dans la mesure où un site piraté peut renvoyer des logiciels malveillants aux internautes le consultant. La deuxième étape est de sauvegarder tous les journaux, les données et programmes du site ainsi que la base de données, avant de procéder à une analyse du système pour connaître l'origine de l'attaque. Cette analyse est primordiale pour une remise en production du site. Elle permet de connaître par quel moyen les attaquants sont entrés dans le système et ce qu'il faut mettre à jour. Le mieux est de revenir sur une version de sauvegarde dont on est sûr qu'elle n'a pas été affectée par la compromission et de la mettre à jour. Parallèlement, il est également vivement conseillé de porter plainte afin que ces attaques soient référencées par les autorités et que des mesures soient prises.

S'il est crucial de prendre en compte la problématique de sécurité lors de la création d'un projet informatique, il est tout aussi indispensable d'en assurer la maintenance afin d'anticiper les attaques et de pouvoir les gérer efficacement, et ainsi minimiser leur impact sur l'activité de l'entreprise.

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

Contactez-nous

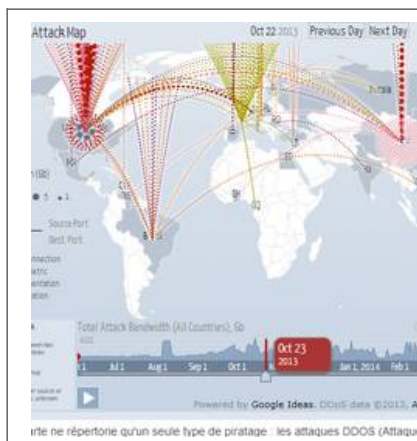
Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire.

Source : <http://www.journaldunet.com/solutions/expert/60882/attaques-informatiques-decryptage-du-phenomene-et-reflexes-a-adopter.shtml>

Par Sébastien Delcroix – NFrance

Cybercriminalité – Retour sur les principales attaques informatiques en France et dans le monde | Denis JACOPINI



Cybercriminalité – Retour sur les attaques informatiques en France et dans le monde qui ont fait la une

Selon la commission européenne, la cybercriminalité englobe 3 catégories d'activité criminelles :

1) Les atteintes directes à des systèmes informatiques (ou Système de traitement automatisé de données, ou encore S.T.A.D.) en perturbant leur fonctionnement, tels que les attaques par déni de services (appelé aussi denial of service attack ou aussi DOS) destinées à faire tomber un serveur (comprenez rendre inaccessible ou mettre en panne un serveur) à distance.

2) Réaliser des actes illicites en utilisant les outils numériques (escroqueries, vols de données bancaires ou personnelles, espionnage industriel, atteinte à la propriété intellectuelle, sabotage, accès frauduleux, fraudes, usurpation d'identité, phishing, création de PC zombies, contamination d'autres postes informatiques ou d'autres serveurs...)

3) Modifier le contenu d'un espace numérique pour y déposer ou diffuser des contenus illicites (pédopornographie, racisme, xénophobie).

Les cyberdélinquants n'ont d'autre objectif que de gagner beaucoup d'argent. Virus, spams, et autres botnets drainent plusieurs centaines de millions de dollars chaque année à travers le monde.

Sans nous étaler sur les 144 milliards de courriers électroniques qui transitent dans le monde chaque jour dont 70% ne sont que du spam, les 10 millions de français victimes d'actes cybercriminels et 75% de ces actes de cybercriminalité qui sont de grande envergure (Norton 2013) qui concernent les 3,2 milliards d'internautes dans le monde en 2014 (dont la moitié pour l'Asie), vous trouverez ci-dessous, par

ordre anté-chronologique, quelques principaux actes cybercriminels recensés par notre Expert, Denis JACOPINI.

Vous pouvez directement contacter Denis JACOPINI ici

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



[Contactez-nous](#)

30/09/2015 : Les sites Web du gouvernement thaïlandais
attaqués
Consulter

12/09/2015 : Cyberattaque contre le site officiel de la
Commission électorale centrale (CEC) de Russie
Consulter

05/08/2015 : La SNCB victime d'un piratage
Consulter

25/07/2015 : Le Pentagone visé par une cyber-attaque russe
Consulter

28/07/2015 : Les e-mails de hauts gradés de l'armée américaine piratés
Consulter

18/07/2015 : Piratage du site de rencontres adultères Ashley Madison
Consulter

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »
« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

06/07/2015 : Hacking Team, société d'espionnage informatique hacké
Consulter

19/05/2015 : Un hacker a modifié en vol la puissance d'un réacteur

[Consulter](#)

14/05/2015 : Un ordinateur de Merkel touché par la cyberattaque contre le Bundestag

[Consulter](#)

14/05/2015 : Des hôtels suisses victimes d'un piratage informatique

[Consulter](#)

12/05/2015 : Kaspersky annonce être victime d'une Cyberattaque

[Consulter](#)

05/05/2015 : Arnaque aux faux virement : Vol de 15 millions d'euros à Intermarché

[Consulter](#)

29/04/2015 : Des pirates informatiques volent 5 millions de dollars à Ryanair

[Consulter](#)

10/04/2015 : Lufthansa victime d'une cyberattaque

[Consulter](#)

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »
« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



[Contactez-nous](#)

05/05/2015 : Les états -Unis (Office of Personal Management) victime de piratage. Plus de 4 millions de données personnelles de personnels fédéraux piratées;
Consulter

09/04/2015 : Arte victime d'une attaque informatique
Consulter

08/04/2015 : La chaîne TV5 Monde victime d'un piratage de grande ampleur par des individus se réclamant du groupe Etat Islamique | Le Net Expert Informatique
Consulter

02/2015 : Thales aurait été la cible d'une cyberattaque

Consulter

02/01/2015 : Les données de deux millions d'abonnés du site de TF1 ont été piratées. Les hackers détiennent les RIB et autres informations sensibles de ces internautes.

Consulter

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

26/12/2014 : PlayStation et Xbox victimes d'une panne après une cyber-attaque. Les joueurs de Xbox (ci-dessus) et de Playstation ne peuvent actuellement plus connecter leur console aux services en ligne en raison d'un piratage.

Consulter

21/12/2014 : Des documents internes de Korea Hydro & Nuclear Power Co. (KHNP), notamment des plans de réacteurs nucléaires sud-coréens, ont été dérobés et publiés de nouveau vers 1h30

ce dimanche sur Internet, pour la quatrième fois depuis le 15 décembre.

Consulter

19/12/2014 : Le régulateur mondial d'internet, l'Icann, a annoncé que des pirates informatiques avaient réussi à pénétrer dans ses ordinateurs.

Consulter

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

18/12/2014 : Une usine métallurgique allemande a subi une cyberattaque qui a provoqué des dégâts matériels conséquents, a révélé jeudi la publication d'un rapport gouvernemental allemand, cité par le site ITworld.

Consulter

18/12/2014 : L'ICANN (Le régulateur mondial d'Internet)

victime d'un piratage informatique

Consulter

21/10/2014 : Staples a annoncé mener une enquête concernant un possible piratage de cartes de paiement, le numéro deux mondial des articles de bureau allongeant ainsi potentiellement la liste des entreprises américaines visées par une cyber-attaque.

Consulter

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

14/10/2014 : Le service de stockage de documents a pris les devants et réinitialisé les comptes utilisant les informations volées. Il affirme ne pas avoir subi d'intrusion sur ses serveurs.

Consulter

02/10/2014 : JP Morgan Chase a indiqué que 76 millions de foyers et 7 millions de PME parmi ses clients avaient été piratés lors d'une attaque informatique dans le courant du mois d'août.

Consulter

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

08/09/2014 : Home Depot : finalement 56 millions de cartes bancaires piratées

Consulter

16/06/2014 : Payer une rançon ou voir les données de centaines de milliers de ses clients publiées sur Internet. C'est le choix auquel devait faire face jusqu'à lundi 16 juin au soir l'entreprise de livraisons de pizzas Domino's Pizza.

Consulter

21/05/2014 : Victime d'une attaque, eBay demande à ses utilisateurs de changer de mot de passe

Les vols de données se suivent et se ressemblent (Target, Orange...). Le spécialiste de l'e-commerce, eBay, vient de communiquer sur une attaque informatique qui aurait visé ses bases de données.

[Consulter](#)

20/05/2014 : Malware BlackShades : 100 arrestations dont 29 en France

A l'origine de l'infection de plus de 500.000 ordinateurs, le logiciel espion BlackShades a donné lieu à une opération de police internationale. En France, 29 personnes ont été placées en garde à vue, en majorité des adolescents ayant avoué avoir exploité le malware.

[Consulter](#)

15/04/2014 : Les deux premiers sites internet reconnaissant avoir subi une attaque liée à la Faille Heartbleed

Au Royaume Uni, le site parental Mumsnet a été attaqué via la vulnérabilité Heartbleed.

Au Canada, l'administration fiscale CRA a admit publiquement avoir été victimes de la faille de sécurité découverte dans l'outil de chiffrement OpenSSL. (900 numéros d'assurance sociale volés) .

[Consulter](#)

12/02/2014 : Une attaque par déni de service (DDoS) a frappé de multiples serveurs aux Etats-Unis et en Europe en début de semaine. Il s'agit de l'attaque informatique de ce type la

plus grande recensée à ce jour.

Consulter

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »
« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

31/01/2014 : La messagerie de Yahoo! victime d'une attaque informatique massive

Des cybercriminels se sont introduits dans des comptes email, à la recherche de données personnelles. Les utilisateurs impactés sont invités à modifier leur mot de passe.

Consulter

27/11/2013 : La chaîne américaine de grande distribution Target a été victime de pirates informatiques qui se sont procuré les coordonnées bancaires de plus de 40 millions de ses clients entre le 27 novembre et le 15 décembre. Ce piratage tombe mal en pleine période des fêtes et ses conséquences sont potentiellement désastreuses pour les

clients ainsi que pour la marque.

[Consulter](#)

28/04/2013 : L'auteur présumé de la cyberattaque contre Spamhaus arrêté

Un Néerlandais de 35 ans a été interpellé en Espagne. Il est soupçonné d'être à l'origine d'une cyberattaque fin mars contre une entreprise basée en Suisse, Spamhaus, qui fournit aux messageries des listes permettant de bloquer les mails indésirables – les fameux spams.

[Consulter](#)

15/02/2013 : Facebook a subi une attaque informatique « sophistiquée »

Le réseau social Facebook a annoncé avoir subi, le mois dernier, une attaque informatique « sophistiquée », qui n'aurait toutefois pas compromis les données de ses utilisateurs.

« Nous avons remédié au problème dans tous les appareils infectés, nous avons informé la police et commencé une vaste enquête qui se poursuit à ce jour », a ajouté le réseau.

[Consulter](#)

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

02/02/2013 : Twitter touché par des attaques informatiques
Le réseau social Twitter a annoncé, vendredi 2 février, que certains de ses utilisateurs avaient été victimes d'attaques informatiques similaires à celles portées contre des sociétés et des médias américains.

Consulter

28/12/2012 : Le groupe pétrolier d'Arabie Saoudite Aramco a révélé avoir fait l'objet d'une attaque informatique de grande ampleur au milieu du mois d'août. Ce sont ainsi 30.000 postes de travail de l'entreprise qui ont été infectés par un virus informatique, provenant de l'extérieur.

Consulter

21/08/2012 : Le nouveau virus Shamoon illustre une fois de plus la progression des attaques visant de 'nouvelles'

cibles. Le virus Shamoon (ou Disttrack) semble écraser des fichiers dans les PC Windows, puis les 'master boot records'. Il en résulte que ces fichiers ne peuvent être récupérés. Or le PC ne peut être redémarré sans qu'ils soient réinstallés.

Consulter

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

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

29/05/2012 : Flame, le virus le plus puissant de l'histoire du cyber-espionnage ?

Découvert au Proche-Orient, ce malware circulerait depuis plus de cinq ans et viserait, comme Stuxnet, des entreprises sensibles et des sites académiques. Une nouvelle arme pour la cyber-guerre ?

Consulter

27/04/2011 : Sony s'est fait pirater en mai 2011 12700 numéros de cartes de crédit non américaines issues d'une vieille base de données.

Consulter

07/03/2011 : Bercy et plus précisément **la direction du Trésor victime d'une vaste opération de piratage** informatique

Au total, plus de cent cinquante ordinateurs du ministère ont été infiltrés et de nombreux documents piratés. La méthode des espions est classique : à partir d'une adresse e-mail piratée, le « hacker » prend le contrôle de l'ordinateur de sa cible grâce à un cheval de Troie, en l'occurrence une pièce jointe. Chacun de ses correspondants au sein de l'administration peut à son tour être infiltré.

Ingénierie sociale a encore frappé. Crédulité ou excès de confiance ?

Consulter

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

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

21/11/2010 : Quand le piratage informatique s'en prend au Nucléaire

Les experts sont maintenant convaincus que le virus Stuxnet a été conçu pour s'attaquer aux centrifugeuses de Natanz utilisées par Téhéran pour enrichir l'uranium.

Consulter

Pour combattre cela, les états organisent 3 branches : Cyberdéfense (atteinte à la sécurité nationale), Cybersécurité (anticipation des risques numériques) et Cybercriminalité qui est la délinquance transposée dans le monde numérique.

Des organismes sont créés ou réorganisés et des hommes embauchés :

O.C.L.C.T.I.C. : Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

D.C.R.I. : Direction centrale du Renseignement intérieur qui depuis début Mai 2014 d'appelle :

D.G.S.I. : Direction Générale de la Sécurité Intérieure

Gendarmerie Nationale

A.N.S.S.I : Agence Nationale de la Sécurité des Systèmes d'Information (créé en juillet 2009)

Cyberdouanes

B.E.F.T.I. : Brigade d'enquête sur les Fraudes aux Technologies de l'Information

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

La webcam, Est-ce une vraie menace pour les utilisateurs d'ordinateurs

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



La webcam,
est-ce une
vraie menace
pour les
utilisateurs
d'ordinateurs

Après Mark Zuckerberg et sa webcam masquée par du scotch, voilà que c'est le directeur de la FBI, James Comey, qui admet avoir adopté le même réflexe.

Une webcam cachée pour s'éviter bien des ennemis

A l'heure où les hackers multiplient les attaques contre les machines des entreprises et des particuliers, beaucoup se sont moqués de Mark Zuckerberg et de son bout de scotch sur la webcam et sur la prise jack, certains allant même jusqu'à le traiter de « parano ». Pourtant, il semblerait qu'il s'agisse d'un réflexe à prendre et ce pour tout le monde. En effet, un pirate talentueux peut assez simplement prendre le contrôle d'une webcam à distance et pousser ainsi l'utilisateur à télécharger un malware sur sa machine. Aussi, lors d'une interview, James Comey, le directeur de la FBI, a défendu l'idée de masquer la webcam. Il a même précisé que ce devait être un réflexe de base en matière de sécurité. En prenant le contrôle de votre caméra, un pirate peut effectivement visionner vos saisies sur clavier et récupérer ainsi identifiants, mots de passe et coordonnées bancaires pour ne citer qu'eux...[lire la suite]

Conseils de Denis JACOPINI

Certes, je recommande toutefois de masquer votre webcam car, même si, en l'absence de logiciel de sécurité adapté, le pirate peut la mettre en fonction sans que vous vous rendez compte de rien. Le pirate peut en effet voir votre tête en train de taper au clavier ou de jouer (ce qui en soit n'aura rien d'intéressant) mais selon l'orientation, voir le reste de la pièce lorsque vous vous éloignez de l'ordinateur. **Mais avez-vous pensé à protéger votre microphone ?** A l'instar des baby phones piratés, mettre en route à distance le microphone de votre ordinateur est tout aussi facile que de mettre en route votre webcam et même mieux d'ailleurs, car à ma connaissance, il n'existe pas de logiciel de sécurité qui empêche l'accès au microphone. Certes tout le monde n'est pas Mark Zuckerberg, mais tout professionnel devrait en plus de couper son téléphone pendant les réunions, penser aussi à boucher le microphone de son appareil ou mieux, enficher une fiche Jack vide. [block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Pion) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaqes dont chacun peut être victime. Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées. Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'aider tous ceux qui se posent la question : Et si ça m'arrivait un jour ? Plutôt que de présenter une longue liste d'arnaqes Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaqes Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques. Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître ! Commandez sur Fnac.fr

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAIM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur CB avec Valérie BENHAIM et ses invités. Commandez sur Fnac.fr

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger" Comment se protéger des arnaques Internet Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière. Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel. J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données). Commandez sur Fnac.fr

Original de l'article mis en page : La webcam, une vraie menace pour les utilisateurs d'ordinateurs

Comment retirer des publications gênante sur les réseaux sociaux ? Les conseils de la CNIL

LE NET EXPERT
AUDITS & EXPERTISES

LE NET EXPERT
EXPERTISES DE SYSTEMES DE
VOTES ELECTRONIQUES
fr

LE NET EXPERT
RGPD
CYBER
MISES EN CONFORMITE

SPY DETECTION
Services de détection
de logiciels espions

LE NET EXPERT
FORMATIONS

LE NET EXPERT
ARNAQUES & PIRATAGES

Denis JACOPINI
vous informe

**Comment retirer
des publications
gênante sur les
réseaux sociaux
? Les conseils
de la CNIL**

Sur les réseaux sociaux, vous pouvez être confronté à la diffusion d'informations personnelles publiée par d'autres internautes. Voici quelques liens utiles pour demander rapidement l'effacement de ces contenus

Une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable ». Sur une publication, vous pouvez être identifié :

- **directement** (exemple : nom, prénom, etc.)
- ou **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à votre identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi votre voix ou votre image).

Votre identification peut être réalisée :

- **à partir d'une seule de vos données** (exemple : numéro de sécurité sociale, etc.)
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

Avant de demander la suppression du contenu, assurez-vous que le compte ou l'information n'appartient pas à un homonyme.

En cas de doute raisonnable, le réseau social peut être en mesure de vous demander tout document permettant de prouver que ce contenu vous concerne. En revanche, **il ne peut pas vous demander des pièces justificatives qui seraient abusives, non pertinentes et disproportionnées par rapport à votre demande.**

1. Signaler la publication à effacer

En fonction du réseau social, vous devez vous rendre sur la page appropriée qu'il a mis à votre disposition à cet effet.

Twitter : Signaler la divulgation d'informations privées

Instagram : Signaler une photo ou vidéo pour violation de vos droits de confidentialité sur Instagram

Facebook : Utiliser le lien » Signaler «

situé à côté de la publication, de la photo ou du commentaire

Snapchat : Signaler la publication ou Utiliser ce formulaire en ligne ou Utiliser le formulaire de droit à l'image

LinkedIn : Signaler le harcèlement d'un utilisateur ou un problème de sécurité

Youtube : Réclamer une atteinte à la vie privée

Dailymotion : Sous chaque vidéo figure un bouton » Signaler cette vidéo »

en cliquant dessus, vous aurez à remplir un formulaire.

2. Si le réseau social ne fait pas partie de cette liste

- Rendez-vous vous en bas de la page d'accueil du réseau social ;
- Identifiez une page « politique de confidentialité » ou « données personnelles » ou « vie privée » ;
- Dans cette page, recherchez les coordonnées du service ou le formulaire qui répondra à votre demande ;
- Envoyez si besoin un modèle à personnaliser qui comprend les références aux textes de loi et vous permet d'indiquer un motif.

Quelle réponse attendre du réseau social ?

Le réseau social doit procéder à l'effacement dans les meilleurs délais et au plus tard dans un délai d'un mois, qui peut être porté à trois mois. Dans ce dernier cas, l'organisme doit vous informer des raisons de cette prolongation dans le délai d'un mois.

En parallèle de cette démarche d'effacement – et si ce contenu est référencé dans les moteur de recherche – exercez votre droit au déréférencement de manière à ce que ce contenu ne soit plus associé à votre nom et prénom dans les résultats d'un moteur de recherche.

En cas de réponse insatisfaisante – ou d'absence de réponse sous un mois – de la part du réseau social ou du moteur de recherche, vous pouvez saisir la CNIL.

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Publication gênante sur les réseaux sociaux : signalez pour supprimer ! | CNIL*

Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité | Denis JACOPINI



Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité

La sensibilisation et l'éducation des utilisateurs jouent un grand rôle dans la réduction des risques.

Il importe donc pour les entreprises d'encourager leurs collaborateurs à se comporter de manière cohérente, en respectant des processus et procédures communiqués clairement, dont la conception et la surveillance sont centralisées et qui couvrent la totalité des équipements en usage. Cela n'évitera peut-être pas toute tentative d'attaque mais renforcera certainement la sécurité de l'entreprise.

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

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI et

<http://www.globalsecuritymag.fr/Les-entreprises-revoient-leur,20150826,55304.html>

Nos ordinateurs ont-ils la mémoire courte ? Vidéo



Nos
ordinateurs
ont-ils la
mémoire
courte ?
Vidéo

Que trouveront les archéologues du futur, d'ici quelques siècles ou quelques milliers d'années ? Des pierres taillées du paléolithique, des hiéroglyphes, des rouleaux de parchemins probablement, des livres peut-être.

Quelles images, quels sons, quels écrits de notre société restera-t-il dans 2000 ans ? Auront-ils résisté aux épreuves du temps et aux mutations technologiques comme l'ont fait la première photo, le premier film, le premier enregistrement sonore. Mais que deviendront les milliards d'informations engrangées dans les disques durs qui se démagnétisent, et sur les CD ou DVD, qui redoutent la lumière du soleil ? [lire la suite]

LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGPD / CNIL**
- **AUDIT RGPD ET CARTOGRAPHIE** de vos traitements
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
- **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité, Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- **Accompagnement** à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- **Audits Sécurité** (ISO 27005) ;
- **Expertises techniques** et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;

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

[Contactez-nous](#)



Régissez à cet article

Source : Nos ordinateurs ont-ils la mémoire courte ?

Mise en conformité RGPD : Accompagnement personnalisé par des Experts

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <i>.fr</i></p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
--	---	--	--	---	---



RGPD
LeNetExpert

**Mise en conformité RGPD :
Accompagnement personnalisé par
des Experts**

Vous souhaitez assister en présentiel pour le RGPD (peut-être un peu par obligation) et vous souhaitez nous faire part d'un projet. Nous vous remercions pour votre confiance.

Informé(e) sur des missions RGPD depuis 2017, après avoir identifié différents types d'activités, nous avons adapté nos offres pour qu'elles correspondent au mieux à vos besoins.

1. Nos interventions d'expertise :
Nous pouvons vous accompagner pour appréhender l'essentiel de la réglementation Européenne relative à la Protection des Données à Caractère Personnel et le nécessaire pour comprendre et observer une mise en conformité, que soit la formation ad-hoc, vous êtes actives mais pouvez toujours compter sur notre soutien soit sous forme de formation personnalisée, soit sous forme d'accompagnement personnalisé ;

2. Nos webinaires : Nous pouvons vous accompagner pour la mise en place de la mise en conformité ;

3. Nos ateliers : Nous pouvons vous accompagner pour la mise en place de la mise en conformité de votre établissement avec le RGPD (Règlement Général) sur la Protection des Données ;

4. Nos ateliers : Nous pouvons vous accompagner pour la mise en place de la mise en conformité de votre établissement avec le RGPD (Règlement Général) sur la Protection des Données ;

5. Nos ateliers : Nous pouvons vous accompagner pour la mise en place de la mise en conformité de votre établissement avec le RGPD (Règlement Général) sur la Protection des Données ;

Après de vous avoir une présentation personnalisée adaptée à la fois aux besoins de votre structure, conforme à votre stratégie et à vos priorités, nous discuterons que vous répondiez à nos questions.

Nous vous garantissons une confidentialité extrême sur les informations communiquées. Les personnes habilitées à les consulter sont soumises au secret professionnel.

Mon nom / Prénom (obligatoire)

Mon nom / Nom (obligatoire)

Mon adresse de messagerie (obligatoire)

Mon numéro de téléphone (ce sera peut-être utilisé pour le démarchage)

Pouvez-vous nous décrire brièvement votre activité ? (obligatoire)

Remarque : Vous pouvez nous écrire directement un message dans la case « **COMMENTAIRES COMPLÉMENTAIRES DE VOS VOSZ UTILES** ». Néanmoins, si vous souhaitez que nous vous établissions un chiffre précis, nous aurons besoin dans un premier temps des informations ci-dessus.

DES VOSZ VOSZ EN COMPLÉMENT :

1. La découverte de vos obligations : Sapelez-vous découvrir le RGPD et l'essentiel pour comprendre et observer la découverte ? (recommandé)	<input type="checkbox"/>
2. Connaître le RGPD : Il consiste à recevoir un atelier pratique de connaître le RGPD des lois précises afin de faciliter l'analyse réglementaire du contexte et de la mise en conformité de la mise en œuvre des tâches et des données. La suite de la découverte peut être faite à distance.	<input type="checkbox"/>
3. Connaître la mise en conformité : Il consiste à mettre en place des aménagements ;	<input type="checkbox"/>
4. Connaître le suivi de la mise en conformité : Cette phase consiste à maintenir la mise en conformité avec le temps par une mise à jour précise du registre des traitements ;	<input type="checkbox"/>

5. Votre mission consiste à effectuer un accompagnement de professionnels à l'entreprise, à leur préciser dans les commentaires ; ou est-ce l'objectif à votre établissement ?

Commentaires complémentaires de vos vosz utiles :

Mon nom / Prénom (obligatoire)

Mon nom / Nom (obligatoire)

Le nom, prénom et email à adresser à : [contact@vosz.fr]

Denis JACQZ est notre Expert qui vous accompagnera dans votre mise en conformité avec le RGPD



Le nom, prénom et email à adresser à : [contact@vosz.fr]

Je me présente : Denis JACQZ, je suis expert en informatique avancée et spécialiste en RGPD, Protection des Données à Caractère Personnel et en cybersécurité. Consultant depuis 1996 et formateur depuis 2006, j'ai une expérience depuis 2012 dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant OMI (CCI) ; Correspondant Informatique et Libertés puis de formation juridique à la Protection des Données (DPO (DPO)) ; en tant que praticien de la mise en conformité de l'entreprise ; je suis spécialisé dans toutes les questions de mise en conformité avec le RGPD.

Mon objectif est de mettre à disposition toute mon expérience pour mettre en conformité votre établissement avec le RGPD. =