Quelles formalités pour transféret des données personnelles hors UE ? | Denis JACOPINI

Quelles formalités accomplir auprès de la CNIL si vous transférez des données personnelles hors de l'Union européenne ?
Les formalités à accomplir auprès de la CNIL varient en fonction :
• du régime juridique applicable au traitement principal (déclaration normale ou autre formalité),
• de la désignation d'un correspondant informatique et libertés,
• du pays de destination,
• du cadre juridique du transfert.

1.
Certains transferts sont dispensés de déclaration
Les traitements mis en œuvre sur le territoire français par des prestataires agissant pour le compte de responsables de traitement établis hors de l'UE et concernant des données personnelles collectées hors de l'UE sont dispensés de formalité, à condition que les traitements aient pour finalité : la gestion des rémunérations, la gestion du personnel ou la gestion des fichiers de clients et de prospects (Dispense n° 15)

2.
Certains transferts hors UE bénéficient déjà d'une autorisation de la CNIL,
C'est notamment le cas des normes suivantes :
• Norme simplifiée n°NS-046 (gestion du personnel)
• Norme simplifiée n°NS-048 (gestion clients-prospects)
• Autorisation unique n°AU-004 (alertes professionnelles)
• Des transferts bénéficiant d'une autorisation unique BCR

3.
Dans les autres cas
Complétez le formulaire correspondant au régime juridique de formalités CNIL applicable au traitement principal envisagé (déclaration normale ou une autre formalité).
Dans ce formulaire, dans l'onglet « Transferts », sélectionnez « **Transmission de données Hors UE** ».

CADRE JURIDIQUE DU TRANSFERT	SI LE TRAITEMENT PRINCIPAL RELÈVE DE LA DÉCLARATION	SI LE TRAITEMENT PRINCIPAL RELÈVE DE L'AUTORISATION	SI LE TRAITEMENT PRINCIPAL RELÈVE DE LA DEMANDE D'AVIS
Le transfert se fait dans un pays présentant une protection suffisante ou Recours aux exceptions	Remplir le formulaire de déclaration normale et l'annexe transferts Ou si l'organisme a désigné un CIL : Inscription au registre du CIL	Remplir le formulaire de demande d'autorisation et l'annexe transferts	Remplir le formulaire de demande d'avis et l'annexe transferts
Clauses contractuelles types	Remplir le formulaire de déclaration normale et l'annexe transferts Le transfert est soumis à l'autorisation préalable de la CNIL	Remplir le formulaire de demande d'autorisation et l'annexe transferts	Remplir le formulaire de demande d'avis et l'annexe transferts
« Binding corporate rules » (BCR) au sein d'un même groupe	Remplir le formulaire de déclaration normale et l'annexe transferts Le transfert est soumis à l'autorisation préalable de la CNIL	Remplir le formulaire de demande d'autorisation et l'annexe transferts	Remplir le formulaire de demande d'avis et l'annexe transferts

Comment procéder ?
• 1 – Complétez le formulaire
• 2- Sélectionnez les pays destinataires
• 3 – Remplissez l'annexe Transfert
• 4 – L'instruction du transfert par la CNIL

Attention ! si vous transférez des données pour plusieurs finalités distinctes, vous devez créer une annexe pour chaque transfert hors UE.
(ex : finalités d'hébergement de données et finalité de saisie de données = 2 annexes).
En revanche, une seule « annexe transfert » suffit pour plusieurs destinataires dès lors que la finalité du transfert est la même.

Article original de la CNIL

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 : Transferts hors UE : quelles formalités ? | CNIL

4 conseils pour éviter les cyber-attaques pendant les soldes | Denis JACOPINI

4 conseils pour éviter les cyber-attaques pendant les soldes

Période propice aux achats en ligne, les soldes sont aussi prisées par les cybercriminels. Tour d'horizon des mesures à prendre pour se prémunir d'une attaque informatique.

Les soldes d'hiver démarrent aujourd'hui. Période de forte activité, les e-commerçants vont voir leurs ventes augmenter et cela ne manquera pas d'attirer les cybercriminels en tout genre. A cette période, chaque année, les entreprises tout comme les particuliers sont la cible de nombreuses tentatives de piratage, cependant quelques conseils simples peuvent éviter aux particuliers les arnaques.

Pendant un mois les soldes représente un pic d'activité pour les sites d'achats en ligne. Début 2014, selon une étude de la Fevad (Fédération du e-commerce et de la vente à distance) et du CSA, 7 internautes sur 10 envisageaient de préparer ou de faire leurs achats en ligne pendant les soldes. Parmi eux, 26% envisageaient d'effectuer leurs achats via smartphones. L'occasion idéale pour les pirates informatiques en quête de nouvelles victimes !

Pour se prémunir de ces attaques, les internautes peuvent prendre quelques précautions simples mais pourtant essentielles :
1. Veiller à toujours avoir les dernières mises à jour de ses applications, de son système d'exploitation et des logiciels de sécurité. Des failles sont régulièrement enregistrées et les correctifs sont présents dans les mises à jour, mais encore faut-il les effectuer !

2. S'en tenir aux règles d'or : Ignorer ou bloquer les pop-ups, utiliser un mot de passe original et sécurisé (aux oubliettes le 0000 ou le 1234), commander sur des sites fiables et via des connexions sécurisées en https.
3. Eviter de cliquer sur les liens directement depuis un emailing :le phishing reste à la mode, et il est particulièrement efficace en période de soldes lorsque des dizaines d'emails vous propose leurs bons plans quotidiennement. Si une offre est pertinente : mieux vaut retaper l'adresse sur son navigateur afin d'éviter tout soucis.
4. Eviter les transactions depuis des réseaux Wi-Fi publics. La plupart des réseaux publics (gares, cafés, etc) ont un niveau de cryptage faible, et donc une moindre sécurité. Les informations bancaires pourraient atterrir dans les mains d'une tierce personne. Que l'on soit connecté depuis un ordinateur, une tablette, ou un mobile, mieux vaut donc se méfier des réseaux ouverts.

Autre point sensible : Les achats via smartphones et tablettes sont de plus en plus communs, mais il est important de se méfier lors de son shopping. En effet, ces terminaux font face à de nombreuses menaces et sont souvent moins bien sécurisés que les ordinateurs.
Ici aussi des règles d'or s'appliquent : ne pas télécharger d'applications gratuites et de propriétaires inconnus sur internet afin d'éviter les trojans, acheter et visualiser les comptes seulement via des applications propriétaires (celles de sa banque ou celles d'e-commerçants), supprimer l'historique de navigation, le cache et les cookies régulièrement afin de supprimer les données sensibles.

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

Source : http://www.lesechos.fr/idees-debats/cercle/cercle-120665-4-conseils-pour-eviter-les-cyber-attaques-pendant-les-soldes-1080620.php

Formation RGPD pour devenir DPO de votre organisme – Prochaine formation les 17 18 et 19 septembre 2018 à Paris

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

Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Formation pour DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement » : 2 jours (Mettez en place une démarche de mise en conformité RGPD)

Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement.
Consultez les prochaines dates d'animation autour de chez vous ?

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, 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, il m'est ainsi aisé d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.
« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

Votre Prénom / NOM (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (pour faciliter l'organisation)

Vous souhaitez avoir des informations sur :
☐- la formation « Comprendre le RGPD » : 1 jour
☐- la formation « Je veux devenir Délégué à la Protection des Données » 2 jours
☐- la formation « Je mets en conformité mon établissement » 3+1 jours
☐- la formation « Mise en conformité RGPD sur mesure »
☐- un accompagnement personnalisé au RGPD

Vous souhaitez réserver une ou plusieurs place(s) à la formation :

Formation pour TPE/PME : **« Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour DPO : **« Je veux devenir le Délégué à la Protection des Données de mon établissement »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour consultants : **« J'accompagne mes clients dans leur mise en conformité avec le RGPD »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

☐Autre ville ou sujets souhaités en individuel (indiquez ci-dessous)

Votre message avec vos préférences de date ou vos commentaires

Envoyer

Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre acompte. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre acompte sera remboursé en intégralité dans les 5 jours (les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part moins de 48 heures avant la formation, l'acompte pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION
N° DPO-15945

Numéro de formateur
93 84 03041 84
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé et référencé

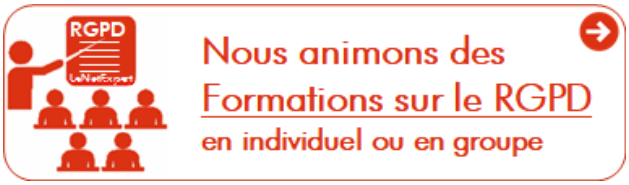
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

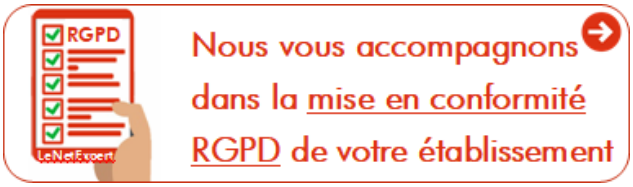
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec 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, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre 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)

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

Source : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*

Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques professionnelles ? | Denis JACOPINI

Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques professionnelles ?

Votre employeur peut mettre en place un dispositif d'écoute ou d'enregistrement des conversations téléphoniques professionnelles.

Ce dispositif doit toutefois prévoir des garanties :

• Écoute ou enregistrement ponctuel, d'une partie seulement des appels;
• Écoute ou enregistrement à des fins d'évaluation, de formation et de contrôle qualité ;
• Information et consultation préalables des instances représentatives du personnel et des employés ;
• Conservation limitée à un an maximum des enregistrements audio ;
• Déclaration à la CNIL du dispositif.

Dans certains cas prévus par un texte légal, des enregistrements permanents peuvent être imposés (services d'urgence ou ordres boursiers, par exemple).

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=ED8EEF20B4B0A650CC53FA8D4DE31A0C?name=Mon+employeur+peut-il+enregistrer+ou+%C3%A9couter+mes+conversations+t%C3%A9l%C3%A9phoniques+professionnelles+%3F&id=269

---

5 règles d'or pour les utilisateurs des réseaux sociaux | Denis JACOPINI

5 règles d'or pour les utilisateurs des réseaux sociaux

Le nombre total d'individus dans le monde est de 7,4 milliards. Fin 2015, Facebook a atteint les 1,59 millions d'utilisateurs. Avec une augmentation annuelle de 17%, le géant des réseaux sociaux est tout simplement trop important pour être ignoré. Ceci étant dit, c'est aussi vrai pour beaucoup d'autres réseaux sociaux.

Les 310 millions d'utilisateurs actifs par mois sur Twitter postent 347 222 fois en moyenne. Plusieurs d'entre eux tweetent plus d'une centaine de fois par jour, et nombreux sont ceux à tweeter une fois par jour. Plus de 40 millions de photos ont été partagées sur Instagram depuis son lancement, et plus de 80 millions de photos y sont publiées chaque jour.
Ceci représente une énorme quantité de données : certaines importantes, d'autres intéressantes ou encore inutiles. Les réseaux sociaux, avec leurs propres tendances et leurs propres lois, fonctionnent comme une extension du monde réel, qui a un énorme impact sur nos vies hors-ligne. Dans cet article, nous vous dévoilons quelques règles simples que chaque utilisateur de réseaux sociaux devrait garder en tête.

1. N'alimentez pas les trolls

Les trolls sur Internet sont des provocateurs qui se joignent à des conversations dans le but d'agacer les autres utilisateurs pour le « fun ». On peut trouver des trolls n'importe où : sur les forums, les chats, et autres plateformes de communication en ligne. Les forums des nouveaux médias sont connus pour la participation élevée de trolls. D'ailleurs, il y en a plein sur les réseaux sociaux.
Comment devez-vous parler aux trolls ? D'aucune façon ! Ignorez-les. Plusieurs personnes se font prendre au piège et engagent alors des débats houleux en essayant d'expliquer leur point de vue et passent une grande partie de leur temps et de leur énergie en vain. Quelqu'un a toujours tort sur Internet. Ne perdez pas votre temps et votre énergie pour des trolls.
View image on Twitter

Si vous n'avez pas de chance, vous pourriez tomber sur un troll en quête de revanche, en spammant votre e-mail, ou même en essayant de ruiner votre vie. Par exemple, un couple américain a perdu du temps, de l'argent, leur travail et même détruit leur mariage en étant les victimes de cybercintimidation, se traduisant par des canulars téléphoniques (swatting) et autres formes d'harcèlement hors-ligne.

2. Ne postez pas ou ne partagez pas de contenu illégal

Les Emirats Arabes Unis et la Nouvelle Zélande disposent de lois qui punissent sévèrement les trolls et la cyberintimidation avec des sanctions allant de 35 000$ à la prison.
Toutefois, vous pouvez écoper d'une amende ou même être confronté à des conséquences bien plus graves pour avoir posté, partagé du contenu ou toutes autres actions relatives dans bon nombre de pays. Par exemple, deux hommes ont été condamnés à quatre ans de prison après avoir créé une page Facebook qui encourageait une révolte. Un homme au Bengladesh a été envoyé en prison pour avoir plaisanté sur son souhait de voir le premier ministre mort.
Par conséquent, mieux vaut être au courant des lois de chaque pays et de s'en souvenir au moment de publier ou partager sur Facebook ou Twitter.

3. Ne partagez pas des arnaques

Les fraudeurs piègent souvent les victimes avec des histoires choquantes telles que des bébés mourants, des chiots qui se noient, ou d'anciens combattants. De tels articles font le tour des réseaux sociaux en criant à l'aide. En réalité, ils sont déployés dans le but de voler de l'argent, de diffuser des malwares et des méthodes d'hameçonnage.
View image on Twitter

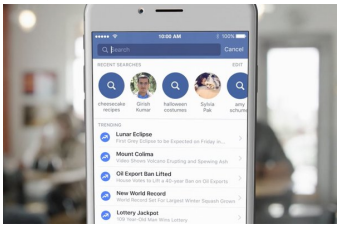
Follow

CityNews Toronto
@CityNews
Consumers warned about online scam involving free puppies **http://ow.ly/YAgcm**
3:14 AM – 22 Feb 2016
*
*
2020 Retweets
*
99 likes

De tels articles génèrent beaucoup de partages, mais la majorité d'entre eux sont des arnaques. De vrais appels au secours proviennent en général de votre famille, amis, et amis de vos amis. Ayez toujours en tête que ce sont les pages officielles des entreprises qui mettent en place ce type d'aide et non pas des individus inconnus.
C'est la raison pour laquelle il vaut mieux rester vigilant et vérifier chaque article avant de cliquer sur « aimer » ou « partager ». Pas envie de tous les contrôler un par un ? Ne prenez donc pas de risques pour vous et vos amis.

4. Pensez aux réactions des lecteurs

Vous avez probablement des collègues, des supérieurs et des clients parmi vos connections Facebook ou Instagram. Lorsque vous postulez pour un emploi, il est très probable par exemple que les ressources humaines jettent un coup d'œil à votre profil sur les réseaux sociaux. Prenez en compte ce que vous voulez leur montrer, et plus important encore, ce que vous ne voulez pas.
Vous devez aussi réfléchir prudemment à ce que vous publiez sur les pages d'autres utilisateurs et sur des comptes publics tels que des entreprises ou des universités. Par exemple, en 2013, un homme originaire de Pennsylvanie ***a été renvoyé pour avoir « complimenté »*** *une étudiante en ligne. Son commentaire n'avait rien de sexuel ou d'inapproprié, mais de toute évidence la mère de la jeune fille n'avait pas apprécié. Un an auparavant, une professeure de Moses Lake, Washington, avait été virée parce qu'une femme qu'elle n'avait jamais rencontrée s'était* ***plainte*** *d'un de ces articles. Il s'agit de quelques exemples parmi tant d'autres qui prouvent qu'il vaut mieux garder ses photos personnelles et ses articles pour des amis sûrs.*
Si vous avez besoin d'aide pour dissimuler vos articles privés des regards indiscrets, vous pouvez retrouver nos articles sur les paramètres de confidentialité de ***Facebook****,* ***Twitter****,* ***Instagram****,****LinkedIn****, et* ***Tumblr****.*
View image on Twitter



Follow

Kaspersky Lab
@kaspersky
Check your Facebook privacy settings NOW **https://kas.pr/3Wpw**
8:13 PM – 26 Oct 2015
*
*
2525 Retweets
*
1313 likes

5. Ne dévoilez pas vos données publiques

De nombreux réseaux sociaux proposent d' « enregister » la géolocalisation lorsque vous prenez une photo, postez du contenu ou montrez les lieux que vous avez visités. Si vous êtes intéressé par un évènement, le réseau social peut en informer vos amis au cas où ils voudraient vous accompagner.
Par défaut, tout le monde peut accéder à vos données, et les cybercriminels ont mille et une méthodes de s'en servir, ça peut aller de s'introduire dans votre maison jusqu'à voler votre identité numérique. C'est la raison pour laquelle nous vous recommandons vivement de dissimuler ce type des données à des personnes inconnues, à l'aide des paramètres de confidentialité de Facebook.
C'est aussi une bonne occasion pour que vous n'ajoutiez pas n'importe qui aveuglément : les gens envoient des demandes d'amis qui peuvent s'avérer être des bots, des trolls ou même des hackers. Même si Facebook vous informe que vous avez des dizaines d'amis en commun, n'acceptez pas de demandes si vous n'êtes pas certain que ce soit des connaissances sûres.
Article original de John Snow

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 : 5 règles d’or pour les utilisateurs des réseaux sociaux | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Recherche de preuves dans les téléphones, smartphones, tablettes, ordinateur PC, Mac… retrouver des documents, photos ou SMS effacés

Recherche de preuves dans les téléphones, smartphones, tablettes, ordinateur PC, Mac… retrouver des documents, photos ou SMS effacés

---

Doutes, soupçons ? Vous pensez que quequ'un vous a volé des données ? Vous pensez que votre conjoint(e) ou enfant a quelque chose à vous cacher ? Vous pensez que le téléphone contient les preuves qu'il vous faut ? Pour mettre un terme à ces interrogations, Denis JACOPINI vous permet une récupération des preuves et un usage judiciaire si vous le désirez.

Denis JACOPINI, Expert de justice en Informatique. Assermenté par les tribunaux, il est inscrit sur les listes des Tribunaux de Commerce, Tribunaux d'Instance, de Grande Instance et Administratif sur les catégories suivantes :

- E-01.02 Internet et Multimédia
- E-01.03 Logiciels et Matériels
- E-01.04 Systèmes d'information (mise en oeuvre)
- G-02 Investigations scientifiques et techniques
- G-02.05 Documents Informatiques (Investigations Numériques)

Diplômé en Droit de l'Expertise Judiciaire, en Cybercriminalité, Certifié en Gestion des Risques sur les Systèmes d »information (ISO 27005 Risk Manager), équipé des meilleurs équipements utilisé en Investigation Numérique par les Polices du monde entier, il vous permettra de retrouver des traces et des preuves dans de nombreux supports (e-mails, fichiers, appels émis, reçus, sms, mms, photos, vidéos etc… même effacés de la quasi totalité des téléphones du marché).

Avec les meilleurs équipements utilisés par les Polices du monde entier, ils est enfin possible de faire parler vos équipements numériques.

Rechercher de preuves dans un téléphone, un smartphone ou une tablette

Vous souhaitez rechercher des preuves dans un téléphone, un smartphone ou une tablette ?
Contactez-vous

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

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (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

ou suivez nous sur

Réagissez à cet article

RGPD : Vous voulez vous mettre en conformité ? Voici comment faire

Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

La mise en conformité est une démarche avant tout réglementaire. Elle doit d'abord commencer par un audit avec de nombreux référentiels relatifs à la protection des données à caractère personnel parfois précédée par une sensibilisation du Responsable de Traitement et de certains de ses salariés (la partie pédagogique de la démarche).
Ensuite, doit suivre la mise en conformité destinée à améliorer l'existant en vue de l'approcher le plus possible des règles.
Enfin, doivent suivre des contrôles réguliers compte tenu que les éléments tels que le contexte, les règles et les risques évoluent sans cesse.

Vous souhaitez faire appel à un expert informatique qui vous accompagne dans la mise en conformité avec le RGPD de votre établissement ?

Je me présente : Denis JACOPINI. Je suis Expert en informatique assermenté et **spécialisé en RGPD (protection des Données à Caractère Personnel) et en cybercriminalité**. Consultant depuis 1996 et formateur depuis 1998, 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 CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données (DPO n°15845), en tant que praticien de la mise en conformité et formateur, je vous accompagne dans toutes vos démarches de mise en conformité avec le RGPD20.

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

Pour cela, j'ai créé des services sur mesure :

Vous souhaitez vous mettre en conformité avec le Règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 (dit RGPD) et vous souhaitez vous faire accompagner. Au fil des années et depuis les mises en conformité avec la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nous avons constaté que les mises en conformité devaient se dérouler (et encore à ce jour avec le RGPD) selon 3 phases principales :

1. « Analyse du contexte » en vue d'établir la liste des traitements et les mesures correctives à adopter ;
2. « Mise en place de la conformité RGPD » avec amélioration des traitements en vue de les rendre acceptables ou conformes. Ceci inclue dans bien des cas l'analyse de risque ;
3. « Suivi de l'évolution des traitements » en fonction de l'évolution du contexte juridique relatif à la protection des Données à Caractère Personnel et des risques Cyber. Ce suivi a pour principal intérêt de maintenir votre conformité avec le RGPD dans le temps.

Pour chacune des phases, nous vous laissons une totale liberté et vous choisissez si vous souhaitez :

- « Apprendre à faire » (nous vous apprenons pour une totale autonomie) ;
- « Faire » (nous vous apprenons et vous poursuivez le maintien de la mise en conformité tout en ayant la sécurité de nous avoir à vos cotés si vous en exprimez le besoin) ;
- ou « Nous laisser faire » (nous réalisons les démarches de mise en conformité de votre établissement en totale autonomie et vous établissons régulièrement un rapport des actions réalisées opposable à un contrôle de la CNIL).

Demandez un devis avec le formulaire ci-dessous

Pour ceux qui veulent apprendre à faire, nous proposons 3 niveaux de formation

1. Une formation d'une journée pour vous sensibiliser au RGPD : « **Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer** » ;
2. Une formation de deux jours pour les futurs ou actuels DPO : « **Je veux devenir le Délégué à la Protection des Données de mon établissement** » ;
3. Une formation sur 4 jours pour les structures qui veulent apprendre à mettre en conformité leurs clients : « **J'accompagne mes clients dans leur mise en conformité avec le RGPD** ».

Afin de vous communiquer une indication du coût d'un tel accompagnement, nous aurons besoin d'éléments sur votre structure : Durée dépendant de la taille, de l'activité et des ressources de votre établissement.

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

N'hésitez pas à nous communiquer le plus de détails possibles, ceci nous permettra de mieux connaitre vos attentes.

Votre Prénom / NOM (obligatoire)

Votre Organisme / Société (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (ne sera pas utilisé pour le démarchage)

Vous pouvez nous écrire directement un message dans la zone de texte libre. Néanmoins, si vous souhaitez que nous vous établissions un chiffrage précis, nous aurons besoin des informations ci-dessous.

Afin de mieux comprendre votre demande et vous établir un devis, merci de nous communiquer les informations demandées ci-dessous et cliquez sur le bouton "Envoyer les informations saisies" en bas de cette page pour que nous les recevions. Une réponse vous parviendra rapidement.

MERCI DE DÉTAILLER VOTRE DEMANDE, VOS ATTENTES...

Votre demande, vos attentes... :

VOTRE ACTIVITÉ

Détails sur votre activité :

Êtes-vous soumis au secret professionnel ? OOui ONon OJe ne sais pas

Votre activité dépend-elle d'une réglementation ? OOui ONon OJe ne sais pas

Si "Oui", laquelle ou lesquelles ?

VOTRE SYSTÈME INFORMATIQUE

Pouvez-vous nous décrire la composition de votre système informatique. Nous souhaiterions, sous forme d'énumération, connaître les équipements qui ont un quelconque accès à des données à caractère personnel avec pour chacun des appareils TOUS le(s) logiciel(s) utilisé(s) et leur(s) fonction(s).
Exemples :
- 1 serveur WEB avec site Internet pour faire connaître mon activité ;
- 1 ordinateur fixe avec ogiciel de facturation pour facturer mes clients ;
- 2 ordinateurs portables dont :
> 1 avec logiciel de messagerie électronique pour correspondre avec des clients et des prospects + traitement de textes pour la correspondance + logiciel de facturation pour facturer mes clients...
> 1 avec logiciel de messagerie électronique pour correspondre avec des clients et des prospects + logiciel de comptabilité pour faire la comptabilité de la structure ;
- 1 smartphone avec logiciel de messagerie électronique pour correspondre avec des clients et des prospects.

Avez-vous un ou plusieurs sites Internet ? OOui ONon OJe ne sais pas

Quel(s) est(sont) ce(s) site(s) Internet ?

Avez-vous des données dans le Cloud ? OOui ONon OJe ne sais pas

Quel(s) fournisseur(s) de Cloud(s) utilisez-vous ?

VOS TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

Si vous avez déjà établi la liste des traitements de données à caractères personnels, pourriez-vous nous en communiquer la liste (même incomplète) ?

DIMENSIONNEMENT DE VOTRE STRUCTURE

Nombre de salariés de votre structure : 0

Parmi ces salariés, combien utilisent un équipement informatique ? 0

Nombre de services** dans votre structure (exemple : Service commercial, service technique...) : 0

Merci d'énumérer les services** de votre structure :

PRESTATAIRES & SOUS-TRAITANTS

Travaillez-vous avec des sous-traitants ? OOui ONon OJe ne sais pas

Merci d'énumérer ces sous-traitants :

Travaillez-vous avec des prestataires qui interviennent dans vos locaux ou dans vos agences ? OOui ONon OJe ne sais pas

Merci d'énumérer ces prestataires :

Avec combien de société(s) d'informatique travaillez-vous ? 0

Merci d'énumérer ces sociétés d'informatique en indiquant les produits ou services pour lesquels elles interviennent et eventuellement leur pays :

VOTRE SITUATION VIS-À-VIS DU RGPD

Votre établissement échange t-il des données avec l'étranger ? OOui ONon OJe ne sais pas

Si oui, avec quel(s) pays ?

Avez-vous déjà été sensibilisé au RGPD ? OOui ONon OJe ne sais pas

Les personnes utilisant un équipement informatique ont-elles déjà été sensibilisées au RGPD ? OOui ONon OJe ne sais pas

Si vous ou vos collaborateurs n'ont pas été sensibilisés au RGPD, souhaitez-vous suivre une formation ? OOui ONon OJe ne sais pas

VOS LOCAUX

L'analyse des conditions de traitements de données dans votre local professionnel ou vos locaux professionnels fait partie de la démarche de mise en conformité.

Disposez-vous de plusieurs bureaux, agences etc. dépendant juridiquement de votre établissement ? OOui ONon

Si "Oui", combien ? 0

Merci de nous indiquer l'adresse ou les adresses de vos agences (et pays si pas en France) du ou des lieux dans lesquels vous et vos éventuels collaborateurs exercez

TYPE D'ACCOMPAGNEMENT SOUHAITÉ

Nous pouvons vous accompagner de différentes manières.
A) Nous pouvons vous apprendre à devenir autonome (formation) ;
B) Nous pouvons vous accompagner au début puis vous aider à devenir autonome ensuite (accompagnement, audit + formation) ;
C) Vous pouvez choisir de nous confier la totalité de la démarche de mise en conformité (accompagnement) ;
D) Nous pouvons vous accompagner de manière personnalisée (merci de nous détailler vos attentes).
Quel type d'accompagnement souhaitez-vous de notre part (A/B/C/D + détails) ?

FIN DU QUESTIONNAIRE

Si vous le souhaitez, vous pouvez nous communiquer des informations complémentaire telles que :
- Nombre d'agences au total (qui dépendent de l'établissement principal = qui n'ont pas leur propre numéro SIRET) ;
- Nombre d'agences au total qui ont pas leur propre numéro SIRET ;
- Nombre d'agences que votre structure a en France ;
- Urgence de votre projet ;
- Toute information complémentaire que vous jugerez utile pour nous permettre de mieux connaître votre projet.

Envoyer les informations saisies

[block id="24086" title="Mentions légales formulaires"]
* = Données à Caractère Personnel
** = Exemple de services : Service commercial, Service technique, Service pédagogique, Service administratif et financier...

A

ou bien, envoyez un e-mail à rgpd[a-ro-ba-se]lenetexpert.fr

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84 — Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE

Datadock — Organisme validé et référencé

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

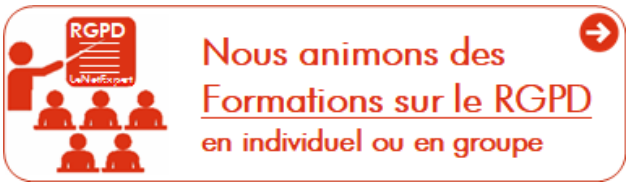
Contactez-nous

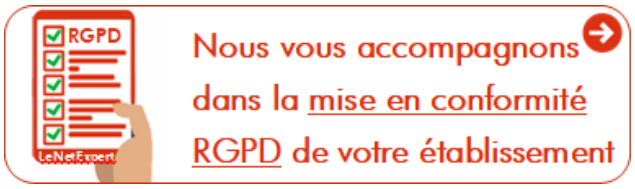
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre 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)

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

Source : Denis JACOPINI

Les conseils de la CNIL pour mieux maîtriser la publication de photos | Denis JACOPINI

10 conseils pour mieux maîtriser sa publication de photos

Les photos occupent aujourd'hui une place centrale dans l'activité numérique des internautes : on les publie, on les partage, on les like, on les commente, on tague ses amis… Elles représentent aussi un véritable enjeu économique pour les acteurs d'internet. Comment mieux maîtriser leur publication ?

1. Adaptez le type de photos au site sur lequel vous les publiez
Certains espaces de publication et partage de photos sont totalement publics et ne permettent pas de restreindre la visibilité des photos. Il est important d'avoir conscience que les photos qui y sont partagées sont alors accessibles à tout le monde et d'adapter le contenu en conséquence.
Evitez d'utiliser la même photo de profil sur des sites ayant des finalités différentes (Facebook, Viadéo ou LinkedIn, Meetic). La photo pouvant être utilisée (moteur de recherche d'images) pour faire le lien entre les différents profils.

2. Limitez l'accès aux photos que vous publiez sur les réseaux sociaux
ll est important de bien définir dans les paramètres de confidentialité quel groupe d'amis a accès à quelle photo ou à quel album photo. Sur Facebook, ce contrôle de l'accès peut passer par la création de liste d'amis et le paramétrage des albums photos ou de chaque photo publiée (voir comment maîtriser les informations publiées sur les réseaux sociaux).

3. Réfléchissez avant de publier une photo
Il n'est pas anodin de publier une photo gênante de ses amis ou de soi-même sur un réseau social. D'autant qu'il peut s'avérer difficile, voire impossible, de la supprimer par la suite (par exemple si elle a été copiée, ou re-partagée par quelqu'un sur le même service ou un autre).

4. Demandez l'autorisation avant de publier une photo de quelqu'un
Il est préférable de s'assurer qu'une photo dans laquelle elle apparaît n'incommode pas une personne avant de la publier.

5. Utilisez avec modération les outils de « tags » (identification) de personnes et la reconnaissance faciale ….
Identifier une personne sur une photo l'expose encore davantage sur la plateforme. Il est donc recommandé de s'assurer que cette identification ne la gêne pas et de restreindre la visibilité de la photo à un cercle de proches.
Attention : cette identification peut être réutilisée par des logiciels de reconnaissance faciale du site qui sont susceptibles du coup d'associer le nom du contact à l'ensemble des photos sur lesquelles il apparait au sein de ce site.

6. Contrôlez la manière dont vous pouvez être identifiés (« taggués ») sur les photos dans lesquelles vous apparaissez et qui sont publiées sur les réseaux sociaux.
Il est possible de paramétrer la façon dont vous pouvez être taggué de manière à :
• Déterminer les contacts ou liste de contacts autorisés à vous identifier ;
• Recevoir une alerte lorsqu'un contact souhaite vous identifier afin de l'approuver (ou non) ;
• Etre alerté lorsque vous êtes identifié dans une photo / publication

7. Faites régulièrement le tri dans vos photos
Contrôler régulièrement qui a accès aux photos que vous avez publiées, en particulier les plus anciennes. Des photos qui semblaient anodines dans un certain contexte, il y a plusieurs années (à une époque où vous aviez moins de contacts, ou une photo publiée pour une occasion spécifique) peuvent s'avérer gênantes aujourd'hui si elles sont accessibles à un cercle de contacts plus large.

8. Faites supprimer les photos qui vous dérangent
Vous avez le droit de faire effacer une photo de vous d'un site ou d'un réseau social. Vous devez demander à la personne qui l'a publiée de l'enlever. Si vous n'obtenez pas de réponse ou si toutes les photos signalées ne sont pas retirées, vous pouvez vous adresser à la CNIL.

9. Faites attention à la synchronisation automatique des photos, en particulier sur smartphone, tablette ou sur les nouveaux appareils photos numériques connectés
Il est recommandé de ne pas activer (ou de désactiver lorsqu'elles sont actives par défaut) les fonctionnalités permettant de synchroniser automatiquement les photos prises avec des services en ligne (« Flux de photos » d'Apple, Instant Upload de Google+ ou Facebook Synchronisation des photos (Photo Sync) par exemple) et de bien réfléchir à leur utilité réelle en cas d'activation. Ces services ne sont pas nécessairement adaptés à une fonction de sauvegarde et de #protection des photos : ce ne sont pas des coffres-forts numériques mais des espaces de partage et publication. Vos photos peuvent n'être alors qu'à un clic d'être rendues publiques. Si ces fonctionnalités peuvent faciliter le partage, elles compliquent encore davantage la suppression des photos.
Même si ces photos ne sont pas automatiquement rendues publiques, elles sont accessibles à l'éditeur du site ou service et pourraient être utilisées par lui pour affiner votre profil, par exemple à des fins publicitaires.

10. Ne partagez pas de photos intimes via votre smartphone !
Ephémère ne veut pas dire sécurisé ! Soyez vigilants si vous utilisez des applications smartphone permettant d'envoyer des photos ou vidéos « éphémères » (Blink, Snapchat, Wickr…). Si l'affichage de la photo est prévu pour durer un temps limité, il est très simple pour le destinataire de conserver une capture d'écran de votre photo. Enfin gardez à l'esprit qu'aucune application smartphone n'est à l'abri d'un piratage, d'un défaut de sécurité ou d'une application tierce malicieuse.

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

Source :
http://www.cnil.fr/linstitution/actualite/article/article/les-conseils-de-la-cnil-pour-mieux-maitriser-la-publication-de-photos/

Quelques préconisations sur la géolocalisation des personnes vulnérables | Denis JACOPINI

Quelques préconisations sur la géolocalisation des personnes vulnérables

Les particuliers, les établissements hospitaliers ou médico-sociaux peuvent aujourd'hui utiliser des appareils de suivi électroniques (bracelets, boîtiers, etc.) pour assurer la sécurité de personnes âgées, malades, ou de jeunes enfants.

Afin de respecter les droits de ces personnes, la CNIL a fait les recommandations suivantes :
• Recueillir si possible l'accord de la personne concernée ou celui de ses représentants légaux ou de ses proches. La personne doit au minimum être informée ;
• Les appareils doivent pouvoir être désactivés et réactivés par les personnes concernées, lorsque celles-ci sont en possession de leurs moyens ;
• La procédure de gestion des alertes doit être précisée dans un protocole ;
• Privilégier les systèmes qui laissent à la personne concernée l'initiative de la demande d'assistance, plutôt qu'une surveillance permanente ;
• S'appuyer sur une évaluation personnalisée des risques et non sur une logique de prévention collective. La géolocalisation ne doit pas être utilisée systématiquement pour toutes les personnes âgées ou tous les enfants accueillis dans un établissement.

Avant de faire le choix d'utiliser ce type d'appareil, une évaluation collégiale et pluridisciplinaire doit donc être menée par l'équipe qui prend en charge la personne vulnérable.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=9DCFCE66E3DC38F485EA18F87E1E023F?name=G%C3%A9olocalisation+des+personnes+vuln%C3%A9rables+%3A+les+pr%C3%A9conisations+de+la+CNIL&id=299

Usurpation d’identité, propos diffamatoires, concurrence déloyale, atteintes à votre E-réputation – Nous pouvons vous aider | Denis JACOPINI

Usurpation d’identité, propos diffamatoires, #concurrence déloyale, atteintes à votre E-réputation – Nous pouvons vous aider

Victime de la cybercriminalité : Quelqu'un vous #insulte sur Internet (propos diffamatoires), se fait passer pour vous (usurpation d'identité sur Facebook, Twitter, viadeo, linkedin, instagram, par e-mail), ou diffuse certaines de vos informations confidentielles, vous pouvez rapidement devenir victime d'une atteinte à votre e-réputation.
Pour initier une action vers la personne malveillante en direction soit d'une arrangement à l'amiable ou d'une action judiciaire, vous devez constituer un dossier avec un maximum d'éléments prouvant la légitimité de votre action.
Denis JACOPINI, Expert Informatique assermenté et spécialisé en protection des données personnelles et en cybercriminalité a rassemblé dans ce document quelques actions qui devront être menées et est en mesure de vous conseiller et de vous accompagner dans vos démarches.

Nous pouvons classer les atteintes à la e-réputation en 3 grandes catégories :

a) Atteintes à la vie privée (par exemple en diffusant ou divulguant des informations personnelles ou confidentielles)
b) Dénigrements, injures, propos diffamatoires, citations hors contextes et médisances
c) Usurpation d'identité
Lors qu'un expert est contacté pour une mission sur un de ces sujets, un constat d'huissier peut éventuellement avoir été demandé, notamment pour constater les faits reprochés. Sans constat, l'expert devra se baser soit sur les informations ou documents que lui communiquera la victime (avec pour issue une vérification de l'exactitude ou de l'intégrité des informations) ou bien procédera à un constat des faits lors de sa mission.

Plusieurs types d'informations peuvent être soumises à l'expert :

Expertiser un e-mail, un post sur un forum, un réseau social ou bien des informations apparaissant sur des supports tels qu'un moteur de recherche, annuaire Internet ou bien un site Internet se fait d'abord en analysant le contexte, puis en réalisant quelques étapes au moyen d'outils spécifiques :

Expertise d'E-mails

En l'absence de procédés de signature électronique garantissant l'intégrité absolue d'un e-mail et de procédé de traçabilité pouvant garantir l'envoi et la distribution dans la boite destinataire d'un e-mail, et, étant quasiment systématiquement dans l'impossibilité de pouvoir expertiser le système informatique à la fois de l'expéditeur et du destinataire, l'expert est souvent bien démuni pour prouver l'absence de fraude dans un « change électronique.
Les premières informations à relever sont bien évidemment la « date de l'e-mail », « l'identité du ou des correspondants » mais aussi une information qui apporte une véracité supplémentaire au mail incriminé : « la continuité des échanges ». (**CAPTURES D'ECRAN DATEE, IMPRESSION DU MAIL**)
La deuxième information très importante est pour les connaisseurs, « l'entête de l'e-mail ». Les informations contenues dans la zone cachée de l'e-mails peuvent certes venir confirmer les informations précédemment relevées, mais également avoir des informations sur les serveurs source, destination et intermédiaires impliqués dans l'échange électronique. (**LA FONCTION D'AFFICHAGE DE L'ENTÊTE D'UN EMAIL FAIT PARTIE DE LA PLUPART DES LOGICIELS DE MESSAGERIE**)
La dernière information pouvant être fort utile consiste à rechercher des informations sur le propriétaire du nom de domaine du serveur à l'origine du message (voir procédure dans la rubrique relative aux expertises de sites internet).
Avec les éléments recueillis, l'expert pourra apporter des éléments permettant à l'avocat d'engager auprès de la personne à qui l'atteinte à la e-réputation est reprochée une demande de réparation à l'amiable ou par voie judiciaire.
Les éléments recueillis permettront, par voie judiciaire, de présenter une requête à un juge, laquelle permettra à l'expert d'obtenir d'autres éléments techniques relatives à l'échange.
Lire notre dossier au sujet des signatures électroniques
http://www.lenetexpert.fr/dossier-du-mois-juin-2014-lutilisation-juridique-documents-numeriques-lere-dematerialisation-outrance/

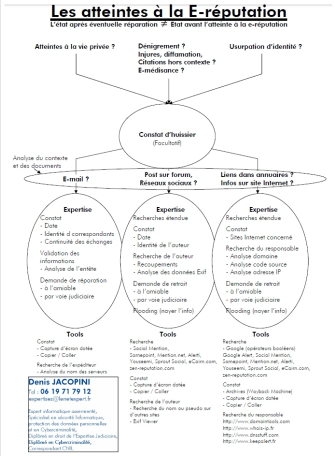
Expertise de post sur forum ou sur les réseaux sociaux ?

Les forums ou les réseaux sociaux peuvent être aussi les dépositaires malgré eux d'échanges ayant pour conséquence l'atteinte à la réputation d'une victime.
Les premières informations à relever sont bien évidemment la « date du message » et « l'identité de l'auteur ». (**CAPTURES D'ECRAN DATEE, CODE SOURCE, ECHANGES AVEC LE FOURNISSEUR DU SERVICE**)
D'autres éléments peuvent nous aider à identifier l'auteur physique d'un message par recoupement d'informations recueillies sur Internet ou dans d'autres sites d'échanges tels que des indices dans les propos ou des informations dans les images utilisées (**recherche sur Google, Social Mention, Samepoint, Mention.net, Alerti, Youseemi, Sprout Social, eCairn.com, zen-reputation.com…**).
Tout comme avec les éléments permettant d'identifier l'expéditeur d'un e-mail, l'expert pourra apporter des éléments permettant d'identifier l'auteur des faits permettant ainsi d'engager seul ou au travers d'un l'avocat, auprès de la personne à qui l'atteinte à la e-réputation est reprochée une demande de réparation à l'amiable ou par voie judiciaire.
Les éléments recueillis permettront, par voie judiciaire, de présenter une requête à un juge, laquelle permettra à l'expert d'obtenir d'autres éléments techniques relatives à l'échange.
Remarque :
En cas de difficulté de faire retirer l'information à l'origine de l'atteinte à la E-réputation, la technique du Flooding peut être utilisée. Elle consiste à noyer l'information par une profusion d'information au contenu cette fois maîtrisé et intelligemment choisi.

Expertise d'informations sur des annuaires ou de sites Internet

Lorsque des contenus portant atteinte à l'E-réputation se trouvent sur des sites Internet, la procédure consiste à identifier le responsable du contenu portant atteinte à la réputation de la victime. Le point d'entrée pour avoir des informations relatives au nom de domaine est principalement le bureau d'enregistrement pouvant nous renseigner sur les coordonnées des différents contacts.
Nous pouvons facilement nous trouver confrontés à plusieurs contacts :
• le contact qui a déposé le nom de domaine
• celui qui a réglé le nom de domaine
• celui qui a ouvert l'hébergement
• celui qui a réglé l'hébergement
• celui ou ceux qui ont mis en ligne le site internet
• celui qui a mis en ligne l'information incriminée
• et enfin l'auteur, et donc responsable, de l'information concernée
Ceci peut représenter autant de contacts pouvant être impliqués ou non dans notre expertise.
Le point d'entrée pour avoir des informations sur ces contacts est principalement le bureau d'enregistrement (Un bureau d'enregistrement (registrar en anglais) est une société ou une association gérant la réservation de noms de domaine Internet).
Nous pouvons avoir plus d'information sur les différents contacts relatifs à un nom de domaine (propriétaire, contact administratif, contact technique) en utilisant la fonction « whois » proposé par les bureaux d'enregistrement ou sur https://www.whois.net.
Voici quelques exemples de registres avec les domaines de premier niveau qu'ils maintiennent :
• VeriSign, Inc. : .com ; .net ; .name
• Public Interest Registry et Afilias : .org ;
• Afilias : .info ;
• CIRA : .ca ;
• DENIC : .de ;
• Neulevel : .biz ;
• AFNIC : .fr ;
• EURid : .eu ;
• Nominet : .uk
Pour pouvez facilement trouver les informations publiques relatives aux noms de domaines grâce aux sites Internet suivants :
• http://www.domaintools.com
• http://www.whois-ip.fr
• http://www.dnsstuff.com
• http://www.keepalert.fr
• http://whois.domaintools.com
Pour information
L'afnic met à notre disposition un formulaire nous permettant de lui demander de procéder à la levée d'anonymat d'un particulier (personne physique), titulaire d'un nom de domaine enregistré sous diffusion restreinte (le nom et les coordonnées du titulaire sont masqués et n'apparaissent pas dans l'annuaire Whois) et sous les extensions opérées par l'AFNIC.
https://www.afnic.fr/medias/documents/RESOUDRE_UN_LITIGE/afnic-formulaire-divulgation-donnees-perso-06-14.pdf
Il est clair que si un prestataire a mis en ligne à la demande de son client les propos concernés par la mission, il devra produire la preuve qu'il a agit à la demande d'un tiers et son identification.
Le code source peut également nous fournir des indications sur le type de logiciel utilisé pour développer le site Internet et le niveau technique du créateur du site Internet.

Enfin, il peut être parfois utile de retrouver le contenu d'un site internet à une date antérieure.
Pour cela, il existe un outil représentant les archives d'Internet : **Internet Archive.**
L'Internet Archive, ou IA est un organisme à but non lucratif consacré à l'archivage du Web et situé dans le Presidio de San Francisco, en Californie. Le projet sert aussi de bibliothèque numérique. Ces archives électroniques sont constituées de clichés instantanés (copie de pages prises à différents moments) d'Internet, de logiciels, de films, de livres et d'enregistrements audio.
Site Internet de Internet Archive : https://archive.org
Accès direct au **WayBackMachine** : http://archive.org/web



Autres délits pour lesquels les Experts Informatiques peuvent être contactés :

Le Cybersquatting
Le Cybersquatting, aussi appelé cybersquattage, est une pratique consistant à enregistrer un nom de domaine correspondant à une marque, avec l'intention de le revendre ensuite à l'ayant droit, d'altérer sa visibilité ou de profiter de sa notoriété.
Parmi les buts recherchés par les cybersquatteurs nous avons :
• Spéculation au nom de domaine
Le cybersquatteur achète un nom de domaine très percutant ou gênant en vue de faire du chantage auprès de l'ayant-droit, pour que celui-ci achète le nom de domaine au cybersquatteur à un tarif élevé.
• Page parking
Le nom de domaine contient des liens sponsorisés qui rapportent des revenus au cybersquatteur. Idéalement, les liens sponsorisés sont en rapport avec le thème de la marque parasitée.
• Boutique d'e-commerce
Le nom de domaine pointe vers une boutique vendant généralement des produits similaires au commerçant dont la marque est cybersquattée. Il s'agit souvent de produits de contrefaçon, le cybersquatteur reprenant les repères visuels de la boutique officielle.
Cette pratique s'apparente au phishing car il s'agit de piéger le consommateur en usurpant l'identité d'un tiers.
• Nuisance à la marque
Le site fait passer un message péjoratif ou dénigrant à l'égard de la marque.
Les actions possibles contre le cybersquattage :
En France, le cybersquattage n'est pas passible de sanctions pénales, seules des actions civiles sont envisageables.
Les actions les plus courantes concernent en atteinte à une marque (propriété intellectuelle) ou encore parasitisme. Des actions peuvent respectivement être portées devant le tribunal de grande instance (TGI) ou le tribunal de commerce dans le cas de conflit entre commerçants.
Procédure extrajudiciaire :
Les organismes qui gèrent les noms de domaines (registres) et les parties prenantes (titulaire du nom de domaine et ayant-droit sur la marque) étant souvent de nationalités multiples d'une part, et les procédures judiciaires étant longues et couteuses d'autre part, l'ICANN a mis au point une procédure extrajudiciaire permettant au plaignant de recourir devant le registre pour récupérer un nom de domaine : la procédure UDRP.
Cette procédure est payante et la décision est à la discrétion du registre. Une décision judiciaire ultérieure prévaudra cependant sur la décision UDRP.

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

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…
Source : http://www.metronews.fr/info/paris-on-refuse-de-lui-louer-un-appartement-a-cause-de-son-profil-internet/modC!uUpMqgL3WsBnc/