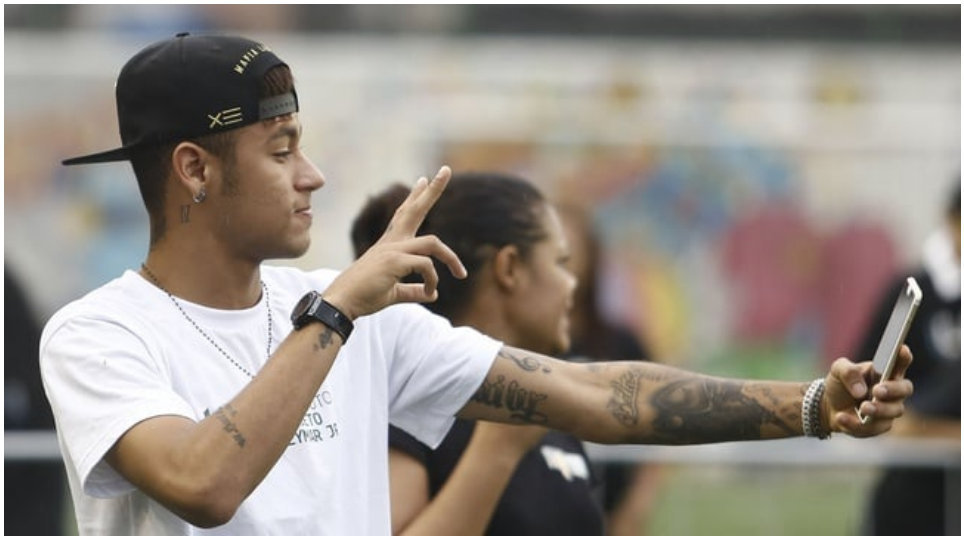
# Vous offrez aux hackers des données invisibles sans le savoir

| | |
|---|---|
|  | Vous offrez aux hackers des données invisibles sans le savoir |

**Empreintes digitales, données GPS des photos, réponses aux questions prétendues «secrètes»…: des données sensibles se cachent sur ce que vous publiez sur les réseaux sociaux, même si l'essentiel du risque se concentre sur des informations livrées plus directement encore…**

Le « V » de la victoire pourrait être celui des hackers. Un chercheur japonais avertissait début janvier contre le danger contenu dans ce signe parfois associé aux selfies: en montrant vos doigts, vous courez le risque de vous faire voler vos empreintes digitales, prévient Isao Echizu.
Alors que les «données sont le pétrole du 21ème siècle », comme on l'entend à l'envi, nous avons une fâcheuse tendance à livrer les nôtres, intentionnellement, sur les réseaux sociaux, en négligeant bien souvent les règles de confidentialité ou l'utilisation commerciale qui est leur est destinée. Mais la vigilance se complique quand on n'a même pas conscience qu'une donnée en est une…

## Attention aux données invisibles…

## Permettez-moi d'emprunter vos empreintes

Avec la haute résolution des photos prises par les smartphones, une opération – assez complexe, toutefois, et loin d'être à la portée de tout le monde – peut permettre de récupérer les empreintes. « Or à l'inverse des mots de passe, les empreintes, une fois volées, ne pourront jamais être changées», rappelle à *20 Minutes* Gérôme Billois, expert cybersécurité au cabinet Wavestone.
Il note que si l'avertissement du professeur japonais a fait le tour du monde, « on connaissait le risque depuis 2014 »: un hacker avait montré lors d'une conférence qu'il était parvenu à cloner les empreintes digitales de la ministre allemande de la Défense. Depuis, les empreintes digitales sont de plus en plus utilisées, pour déverrouiller smartphones, objets connectés ou pour réaliser certains paiements.

## Des photos très bavardes

Autre donnée invisible, la géolocalisation associée aux photos, la grande majorité étant prise aujourd'hui par des smartphones équipés d'une puce GPS (qui ne sert pas qu'à vous guider sur la route jusqu'à Palavas-Les-Flots). Aux images numériques sont associées tout un ensemble de métadonnées, qui «peuvent renseigner la date, l'heure, voire les données GPS de l'image, la marque, le numéro de série de l'appareil ainsi qu'une image en taille réduite de l'image originale», comme le précise We Fight Censorship, qui indique la marche à suivre pour nettoyer ces métadonnées.«Internet abonde de ces images floutées dont le fichier EXIF contient toujours le document avant floutage», lit-on encore.
En septembre dernier, deux étudiants de Harvard ont pu démasquer 229 dealers grâce aux coordonnées géographiques contenues dans les métadonnées associées à des photos qu'ils avaient prises et postées en ligne.

## En huit tweets, tout est dit

Sur Twitter, si la géolocalisation des tweets est désactivée par défaut, beaucoup l'activent. En mai dernier, des experts du MIT et d'Oxford démontraient que huit tweets (d'utilisateurs pour lesquels la géolocalisation est activée) suffisaient à localiser quelqu'un de façon très précise. « Il est extrêmement simple pour des personnes avec très peu de connaissance technique de trouver où vous travaillez ou vivez », expliquaient-ils, à l'issue d'une expérience concluante.

## Le secret imaginaire des questions secrètes

Il y a enfin ces infos que nous livrons publiquement sur les réseaux sociaux alors qu'elles contiennent parfois les réponses aux questions censées être «secrètes». «Les questions secrètes sont le talon d'Achille des réseaux sociaux, souligne Gérôme Billois. Elles vous permettent d'accéder à vos comptes en cas d'oubli de mot de passe et ce sont toujours les mêmes: Quel est le prénom de votre mère? Quel est votre plat préféré? Or toutes ces infos peuvent être retrouvées facilement sur les réseaux sociaux.»

## … et surtout aux données plus évidentes, qui permettent de personnaliser le phishing

Pour les scénarios ci-dessus, qui peuvent avoir le mérite d'attirer l'attention, la probabilité d'utilisation malveillante est pourtant « faible », assure Gérôme Billois. Parallèlement, «nous passons notre temps à livrer des informations hypersensibles», et de façon bien plus directe. Or l'occupation principale des cybercriminels reste les mails de phishing, et ces données les aident à les personnaliser.
«Si le mail est pointu, que c'est votre « bonne » banque qui vous dit qu'elle a remarqué votre passage à telle heure la veille, et que toutes ces infos sont correctes parce que vous avez partagé ces données sur les réseaux sociaux, il y a toutes les chances pour que vous cliquiez sur le lien malveillant.»…[lire la suite]

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits 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.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

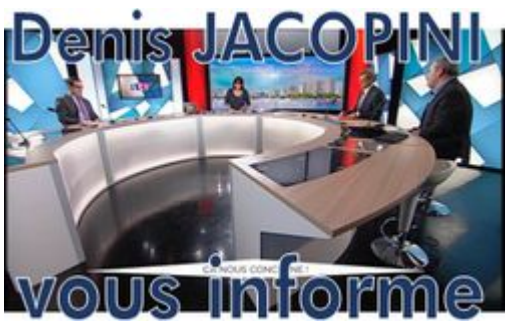
Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Sans le savoir, vous offrez aux hackers des données invisibles

---

# Précautions à prendre avant de se débarrasser du vieux matériel informatique




**Précautions à prendre avant de se débarrasser du vieux matériel informatique**

---

**Lors de la mise au rebut ou de la revente, il est nécessaire de se préoccuper de l'effacement préalable des informations stockées sur tout dispositif comportant un support de stockage (ordinateur, serveur, téléphone, imprimante, clé USB, appareil photo numérique, récepteur GPS).Il est tout aussi important d'appliquer ces règles d'hygiène lors de la réception d'un matériel d'occasion avant sa réutilisation.La méthode choisie pour effacer les informations existantes sur le support informatique obsolète dépend de son niveau de sensibilité et du risque associé (voir Guide technique de l'ANSSI n° 972-1/SGDN/DCSSI). Dans le cas particulier de données ou de matériels protégés par l'instruction générale interministérielle 1300, une procédure stricte doit être appliquée par des personnels habilités. Dans le cas de l'exportation de matériel hors de l'environnement sécurisé de l'entreprise, ou lors d'un transfert interne entre entités ayant des besoins de confidentialité distincts, la mesure la plus sûre reste l'extraction et la destruction physique des supports de stockage, puis leur remplacement lors de la remise en service.Si cette destruction n'est pas envisageable, il existe, pour des composants type PC (comme les disques durs), des logiciels spécialisés destinés à effacer l'intégralité des données stockées. On peut citer le logiciel Blancco, dont la version 4.8 bénéficie d'une Certification de Sécurité de Premier Niveau délivrée par l'ANSSI.**

## Les imprimantes et photocopieurs multifonctions

Les imprimantes et photocopieurs multifonctions se comportent comme un ordinateur en intégrant souvent un navigateur web, une messagerie électronique, une connectivité Wifi et Ethernet, un accès USB et un disque dur. Le fonctionnement standard de ce type de matériel implique de stocker sur le disque dur les documents à imprimer ou à scanner. Selon vos activités ou votre mission, ce disque dur pourrait stocker des données confidentielles de votre entreprise. Un point d'attention particulier doit être porté sur les contrats de maintenance qui intègrent parfois un accès distant non contrôlé à l'équipement depuis Internet.

L'imprimante ou le photocopieur propose souvent des fonctionnalités de sécurité permettant l'effacement du disque dur ou la suppression des données liées aux impressions, copies, télécopies et numérisations pouvant être enregistrées sur le disque dur. Ce processus d'effacement peut parfois être activé automatiquement après chaque utilisation, ou programmé pour s'exécuter à intervalles spécifiés. Ces fonctionnalités ne garantissent pas toujours un effacement sécurisé des données considérées, et les périphériques de stockages internes et externes devront faire l'objet d'une procédure similaire aux autres équipements informatiques avant le décommissionnement de l'appareil. Attention toutefois, ces composants restent généralement la propriété de la société louant les appareils.

Lors de la réception d'un matériel de ce type, il conviendra de désactiver les fonctionnalités de stockage «dans le cloud» lors du paramétrage initial de l'appareil si celles-ci sont disponibles, et de s'assurer du niveau de mise à jour de l'appareil. Il faudra bien sûr maintenir ce niveau régulièrement afin de limiter l'exposition de son système d'information à des failles éventuellement apportées par cet équipement.

## Les autres matériels informatiques

La plupart des matériels modernes intègrent des fonctions de restauration des paramètres d'usine. Il convient a minima de réinitialiser ainsi tout équipement entrant ou sortant de l'entreprise afin de supprimer par exemple certains mots de passes ou autres paramètres de configuration sensibles qui pourraient être stockés sur ces appareils.

Une réinitialisation permet également de se prémunir d'un éventuel piégeage logiciel simple de l'appareil par son précédent propriétaire.

## Documentation

• Guide technique n° 972-1/SGDN/DCSSI : Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter.
http://www.ssi.gouv.fr/archive/fr/documentation/Guide_effaceur_V1.12du040517.pdf
• Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale :
http://www.sgdsn.gouv.fr/IMG/pdf/IGI_1300.pdf
• CSPN du logiciel Blancco :
http://www.ssi.gouv.fr/entreprise/qualification/blancco-data-cleaner-version-4-8/

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits 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..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

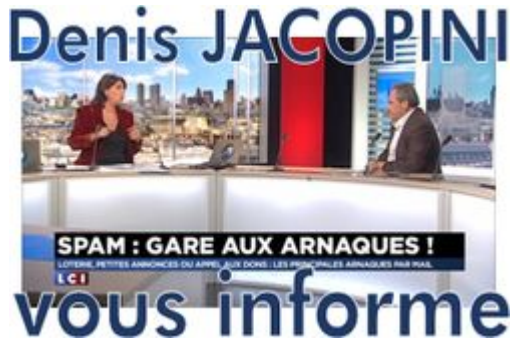
Réagissez à cet article

Original de l'article mis en page : Bulletin d'actualité CERTFR-2017-ACT-007

---

# Une puce RFID sous la peau.

# Des salariés volontaires l’ont essayé…




## Une puce RFID sous la peau. Des salariés volontaires l’ont essayé…

**Une entreprise belge a implanté une puce RFID sous la peau de huit de ses salariés volontaires. Rencontre.**

**Accepteriez-vous de vous faire pucer pour le boulot ?**
C'est ce qu'ont consenti huit des douze salariés d'une agence digitale belge, comme avant eux une entreprise suédoise : mi-décembre, au milieu de leur petit open space blanc et rouge, un pierceur néerlandais leur a logé sous la peau, entre la base du pouce et l'index, une puce RFID (radio frequency identification).
L'une de celles que l'on implante habituellement sous le poil des animaux de compagnie ou des brebis.
Sa silhouette sombre, longue comme un grain de riz, apparaît à travers la chair quand l'un des salariés pucés serre le poing pour nous la montrer.
Comme il l'a fait devant d'autres journalistes avant nous, Tim Pauwels se plie allègrement à la démonstration : sur le trottoir de Malines, ville grise entre Bruxelles et Anvers où l'entreprise est située, il colle avec délicatesse sa main sous l'interphone. Bip!
Miracle tant attendu : la porte s'ouvre. Nous entrons.

**« Adoptons la technologie »**

L'idée de se faire implanter une puce pour ouvrir la porte de leur boîte leur est venue un vendredi. A l'instar des si cool entreprises de la Silicon Valley, les salariés de Newfusion ont chaque semaine « deux heures de libre » dédiées à la cogitation de projets.
Parce que certains oubliaient régulièrement leur clé, ils ont lancé un vendredi le projet de les remplacer par un système électronique de badges. « Plus facile, plus digital », précise dans un anglais fluide Vincent Nys, 27 ans, qui a lancé NewFusion il y a quatre ans.
« On a passé deux jours dessus, on l'a mis en place mais quelques jours plus tard, ils oubliaient leur carte. Alors on a réfléchi : « quelle est la prochaine étape ? » Nous voulions faire quelque chose d'innovant et ouvrir une discussion. »

Une puce RFID et l'un des kits commandés par Newfusion (Emilie Brouze)
En parfaite adéquation avec son époque, Vincent Nys adore l'innovation (il répète le mot à l'envi). Les milliers de personnes dans le monde qui possèdent une puce électronique se divisent à son sens en deux catégories. Ceux qui le font pour se différencier – « être unique, spécial » – et les consommateurs précoces, « comme nous ». Ceux qui n'ont pas peur de se dire :

**« Adoptons la technologie et allons plus loin. »**
Son associé complète :
**« Ceux qui avancent sont ceux qui ouvrent les portes aux autres… Il faut innover pour pouvoir faire des progrès. »**
Innovons donc en ouvrant des portes.

**« Est-ce qu'on le sent ? »**

Avant de commander les puces à une entreprise américaine qui les commercialise en kits stérilisés, il y a tout de même eu discussion au sein de Newfusion. « On a eu un débat, mais pas celui qu'il y a dans les médias », rétorque Vincent Nys :
**« Est-ce que c'est sûr ? Est-ce qu'il y a des implications médicales ? Est-ce qu'on pourra passer un scanner ? Est-ce qu'on le sent ? Est-ce que ça a un impact sur notre vie ? »**
Seulement quatre salariés ont refusé de se faire pucer. « Je ne perds pas mon badge, je n'ai pas vu l'intérêt d'une puce », répond Sam Van Campenhout, développeur.
« Je crois que je n'aimerais pas avoir quelque chose sous ma peau. C'est bizarre », ajoute Sil Colson, jeune designer multimédia.

Sil Colson fait partie des salariés ayant refusé de s'implanter une puce RFID (Emilie Brouze)

Ce qui pourrait la faire changer d'avis ? Que la puce contienne son passeport et qu'il suffise de présenter sa main au moment des contrôles, sans risquer d'oublier ou d'égarer le document en vacances. Ou que la puce contienne les infos essentielles de son carnet médical, immédiatement accessible en cas d'urgence. Pour ouvrir la porte d'entrée, Sil préfère conserver son badge.
Un autre développeur raconte que lui a tout de suite été enthousiaste à l'idée (sa copine un peu moins) : « J'adore la technologie. »
En quelques heures, il a bidouillé un programme que le patron lui demande de nous montrer. Alors Dries Van Craen presse sa main droite contre un boîtier relié à son ordinateur. Bip! (La sonorité est la même qu'à la caisse d'un supermarché.)
S'affiche sur l'écran, sur un fond automnal, un message de bienvenue personnalisé. Sur la colonne de droite sont empilés ses morceaux de musique préférés, au-dessus des temps de transport pour rentrer chez lui, actualisés en temps réel.
Le patron s'enthousiasme :
**« Voilà ce que tu peux faire sans argent et en une demi-journée. Avec des années et une vision, on pourra faire plein de choses. »**
Le jeune patron technophile a installé chez lui un système lui permettant d'ouvrir la porte de son domicile d'un geste de la main.
Prochaine étape : bricoler un moyen de régler son éclairage intérieur grâce à la même puce (un jeu de lumières pour ses soirées en solitaire, un autre quand il est avec sa compagne).

**« Disrupter » le marché**

Quand on lui fait remarquer l'utilité à ce stade toute relative de ces puces sous-cutanées, Vincent Nys assume. Parce qu'il ne s'agit pas que de se débarrasser des badges d'entrée : c'est une piste de développement pour Newfusion.
**« Dans nos têtes, on ne s'est même pas demandé ce qu'on pouvait faire avec [les puces RFID]. On s'est dit « Allons-y, faisons-le ». On ne s'est pas trop préoccupé de questions éthiques, morales et des possibles applications.**
**On pense qu'il faut être les premiers à le faire. On commence par « disrupter » le marché, puis on créé des applications. «**
Sur la RTBF, qui a diffusé l'un des premiers reportages sur l'opération de puçage, Alexis Deswaef, président de la ligue des Droits de l'Homme en Belgique, soulevait une question éthique : « Dans le futur, braderons-nous un peu plus nos droits à la vie privée pour plus de sécurité ou de confort ? »
En dépit des critiques, Vincent Nys, comme son associé, sont ravis des retombées médiatiques, eux qui espéraient intéresser seulement quelques blogs techs avec leur communiqué de presse : on parle d'eux dans le monde entier. Quelle bonne pub ! Des banques, une société de transports publics ou encore une municipalité ont d'ores et déjà pris contact avec eux.

**« Big Brother »**

A côté de ces potentiels nouveaux clients, Newfusion a aussi reçu une cinquantaine de messages désagréables. « Des gens qui faisaient référence aux années Hitler – parce qu'on marquait les gens -, des personnes qui nous traitaient d'antéchrist ou nous parlent de Big Brother… » Beaucoup d'après lui n'ont pas bien compris la technologie.
Vincent Nys fait défiler certains commentaires Facebook sur son téléphone : « Ce n'est pas éthique », « 0% liberté », « il est temps que je lise de nouveau « 1984 » »… Il remarque :
**« Ils sont tous fixés sur ce livre. »**

Vincent Nys, fondateur et directeur de Newfusion, le 9 février 2017 à Malines (Emilie Brouze)
Au début, le patron répondait poliment et pédagogiquement à ceux qui ne sont manifestement pas mûrs pour "aller plus loin" : non, non, non, il ne s'agit pas de traquer les gens. La puce RFID qu'il a lui aussi sous la peau fonctionne sans batterie et ne peut pas transmettre à un tiers la localisation du porteur.
Elle contient un numéro unique ainsi qu'un espace mémoire lui permettant par exemple d'enregistrer sa carte de visite pour la donner à un client en posant sa main sur son smartphone.
Alors oui, le patron peut savoir exactement quand un des employés pucés entre ou sort du bâtiment, « comme avec les badges ou la caméra fixée à l'extérieur », semble-t-il relativiser. « Mais ce n'est pas le but et ce n'est pas notre culture. Les employés ont des horaires de travail souples. »…[lire la suite]

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits 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..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Travailleurs belges pucés : « On ne s’est pas trop préoccupé de questions éthiques » – L’Obs

---

# Le FBI pourra t-il accéder aux mails de Gmail ?

Le FBI pourra t-il accéder aux mails de Gmail ?

---

**Le juge fédéral Thomas Rueter de la cour de Philadelphie a donné son verdict et a statué concernant la saisie de mails depuis des serveurs étrangers, par les autorités américaines. Ce dernier a affirmé : «Même si la récupération de données électroniques par Google à partir de ses multiples centres de données à l'étranger peut en soi représenter un risque d'atteinte à la vie privée, la véritable atteinte intervient au moment de la divulgation aux Etats-Unis».**

En gros, le juge fédéral a estimé que le fait d'ordonner à Google de remettre aux autorités les courriers électroniques de sa messagerie Gmail, stockés à l'étranger, n'était pas contraire à la loi. La firme de Mountain View devra se conformer aux mandats et perquisitions du FBI. Google a évidemment déclaré qu'il faisait appel de la décision, en se référant à la jurisprudence Microsoft, car une affaire similaire avait donné raison à Microsoft il y a quelques semaines à New York.

## Google devra fournir au FBI les mails hébergés à l'étranger

Google ne souhaite pas livrer au FBI les e-mails stockés hors des Etats-Unis, afin de garantir la vie privée de ses usagers aux quatre coins du monde. Sont concernés par la décision du juge fédéral Thomas Rueter, les six serveurs de l'entreprise présents en Belgique, en Finlande, en Irlande, à Taïwan, Singapour et aux Pays-Bas.
Le juge a estimé qu' « *aucune ingérence significative* » avec les droits de propriété du titulaire du compte ne pouvait être invoquée concernant les données ciblées, car comme l'a fait remarquer le juge, Google procède déjà régulièrement au transfert de ces données vers ses serveurs aux Etats-Unis, pour ses propres business et sans que les clients en soient forcément informés. Thomas Rueter de la cour de Philadelphie a souligné : *« Ces transferts n'interfèrent pas avec l'accès du client ou les droits de propriété des données utilisateur. Même si le transfert interfère avec le contrôle du propriétaire du compte sur ses informations, cette interférence est minime et temporaire ».*
Il semble donc que le juge ait retourné les méthodes de Google contre lui-même pour justifier la légalité des saisies des e-mails stockés hors des Etats-Unis au FBI. Du côté de l'entreprise, on s'est contenté de déclarer : *« Nous continuerons à repousser les mandats excessifs ».*

Original de l'article mis en page : Le FBI pourra bien accéder aux mails de Gmail situés à l'étranger

---

A Lire aussi :
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
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
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'audits 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.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

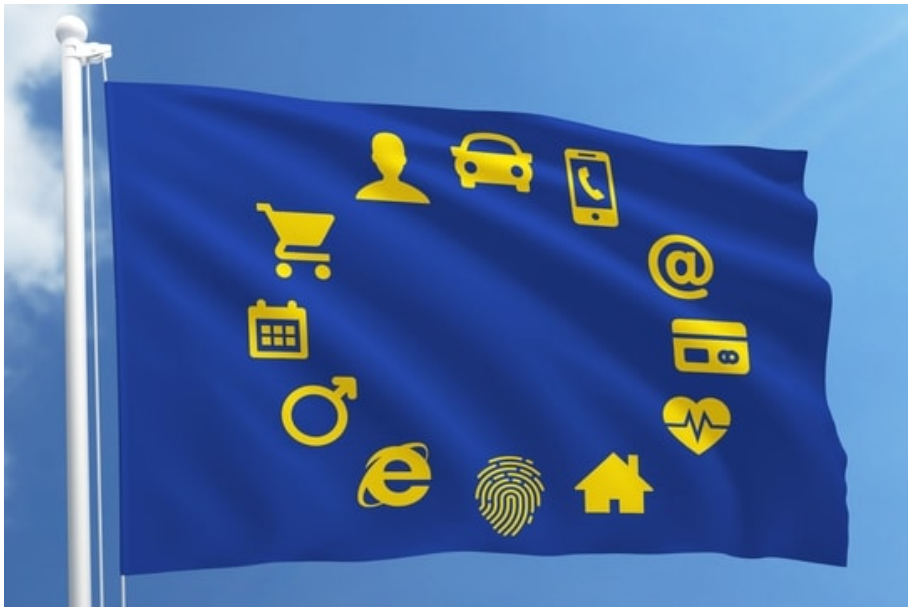
Réagissez à cet article

Original de l'article mis en page : Le FBI pourra bien accéder aux mails de Gmail situés à l'étranger

---

# RGPD Règlement Européen sur la Protection des Données : Voici comment être en règle

# pour 2018

| | |
|---|---|
|  | **RGPD Règlement Européen sur la Protection des Données : Voici comment être en règle pour 2018** |

**Le GDPR, règlement européen qui renforce le droit des utilisateurs en matière de données personnelles, entrera en vigueur en mai de l'an prochain. D'ici là, 4 actions doivent être menées.**

2017 s'annonce chargé pour toutes les entreprises qui collectent et manipulent, de près ou de loin, de la data en provenance de leurs consommateurs. Pour cause, le nouveau règlement européen sur la protection des données personnelles (GDPR) entrera en application le 25 mai 2018. Son objectif est de renforcer les droits des personnes en la matière… et les obligations des entreprises. Voici comment éviter une amende qui sera salée pour les mauvais élèves : 2 à 4% du chiffre d'affaires ou 20 millions d'euros, le montant le plus élevé étant choisi.

## Protéger les données personnelles en amont

Commençons par la bonne nouvelle. L'entreprise qui procède à un traitement de données personnelles n'aura plus à remplir de déclaration auprès de la Cnil pour l'en informer, comme elle y est pour l'instant tenue. Ce pilier de la loi « Informatique et liberté » saute.

« Les entreprises doivent 'en échange' se conformer au concept de « privacy by design » érigé par l'article 25 du règlement », explique Matthieu Berguig, avocat spécialisé en droit des nouvelles technologies. Ce concept leur impose de réfléchir à la protection des données personnelles en amont de la conception d'un produit ou d'un service. « Un fabricant d'objets connectés doit donc se poser des questions de base avant de mettre son produit sur le marché : où son stocké les données, par quel protocole de cryptage seront-elles protégées, sont-elles anonymisées… », illustre Matthieu Berguig. Délestée de ce travail de vérification, la Cnil s'évite beaucoup de paperasse… et gagne du temps pour auditer le marché. « On peut être sûrs que les contrôles seront plus nombreux », prévoit Matthieu Berguig.

## Nommer un déléguer à la protection des données

La Cnil pourra travailler dans cette perspective main dans la main avec un collaborateur d'un nouveau genre, le délégué à la protection des données (DPD). L'article 37 impose sa nomination dans plusieurs cas de figure : lorsque « le traitement est effectué par une autorité publique ou un organisme public », lorsque le traitement impose « un suivi régulier et systématique à grande échelle des personnes concernées » ou lorsque le traitement à grande échelle concerne « les catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10« . Beaucoup d'entreprises sont donc concernées par l'obligation et toutes sont encouragées à en nommer un.

Chargé de faire respecter le règlement européen sur la protection des données au sein de l'organisme qui l'a désigné, le DPD tient un peu du mouton à cinq pattes. Chez les entreprises déjà bien structurées, le « compliance officer », le collaborateur qui s'assure de la conformité de toute décision business à la législation, sera un candidat naturel à ce rôle de DPD. « Pour toutes les autres, il faut trouver la perle rare, un profil juridique capable également de comprendre les problématiques métiers », note Alan Walter, avocat associé chez Walter Billet Avocats.

## Tenir un registre de traitement des données

« En 2017, beaucoup d'entreprises vont s'embarquer dans une totale remise à plat de leurs systèmes de traitement des données à caractère personnel », note Alan Walter. Pour cause, l'article 30 impose aux entreprises de plus de 250 salariés de tenir un registre des traitements effectués. Un registre qui comporte, entre autres, le nom et les coordonnées du responsable du traitement, les finalités du traitement, la catégorie de destinataires auxquels les données à caractère personnel ont été ou seront communiqués. « C'est ce registre qui sera consulté par la Cnil lorsqu'elle voudra entrer en action », précise Matthieu Berguig.

L'article 33 impose d'ailleurs à une entreprise qui a subi une violation de données à caractère personnel d'en notifier l'autorité de contrôle. « Seuls les opérateurs télécoms y étaient jusque-là tenus », note Matthieu Berguig.

## Créer une base interopérable pour le droit à la portabilité

L'article 20 du règlement aboutit à la création d'un droit à la portabilité des données personnelles. Si un de vos clients vous quitte pour la concurrence, il a le droit de réclamer le transfert de l'intégralité des données le concernant. « Lorsque cela est techniquement possible », précise l'article. « En d'autres termes, lorsque vous passerez d'une boîte mail à une autre, vous aurez théoriquement le droit d'importer tout votre historique de mails », illustre Matthieu Berguig. Une obligation dont la mise en place pourrait être techniquement compliquée dans de nombreux cas.

Alan Walter souligne un autre écueil, juridique celui-ci, en prenant l'exemple de l'un de ses clients, courtier en assurance pour expatriés. « Les données qu'il recueille sont très sensibles car elles concernent le domaine médical. Elles ne peuvent être transmises à n'importe qui, du fait du secret médical. Donc comment doit-il faire ? », s'interroge-t-il. Dans ce cas, il faudrait s'assurer que le destinataire des données offre les garanties nécessaires pour qu'il ne soit pas porté atteinte aux droits des personnes concernées. Problématique d'autant plus épineuse avec des transferts de données qui sont susceptibles d'intervenir vers des opérateurs situés hors de l'Union européenne et donc soumis à des droits différents. Premiers éléments de réponse début mai 2018.

Original de l'article mis en page : Protection des données : voici comment être en règle pour 2018

---

A Lire aussi :

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

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 dessins

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'audits 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.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

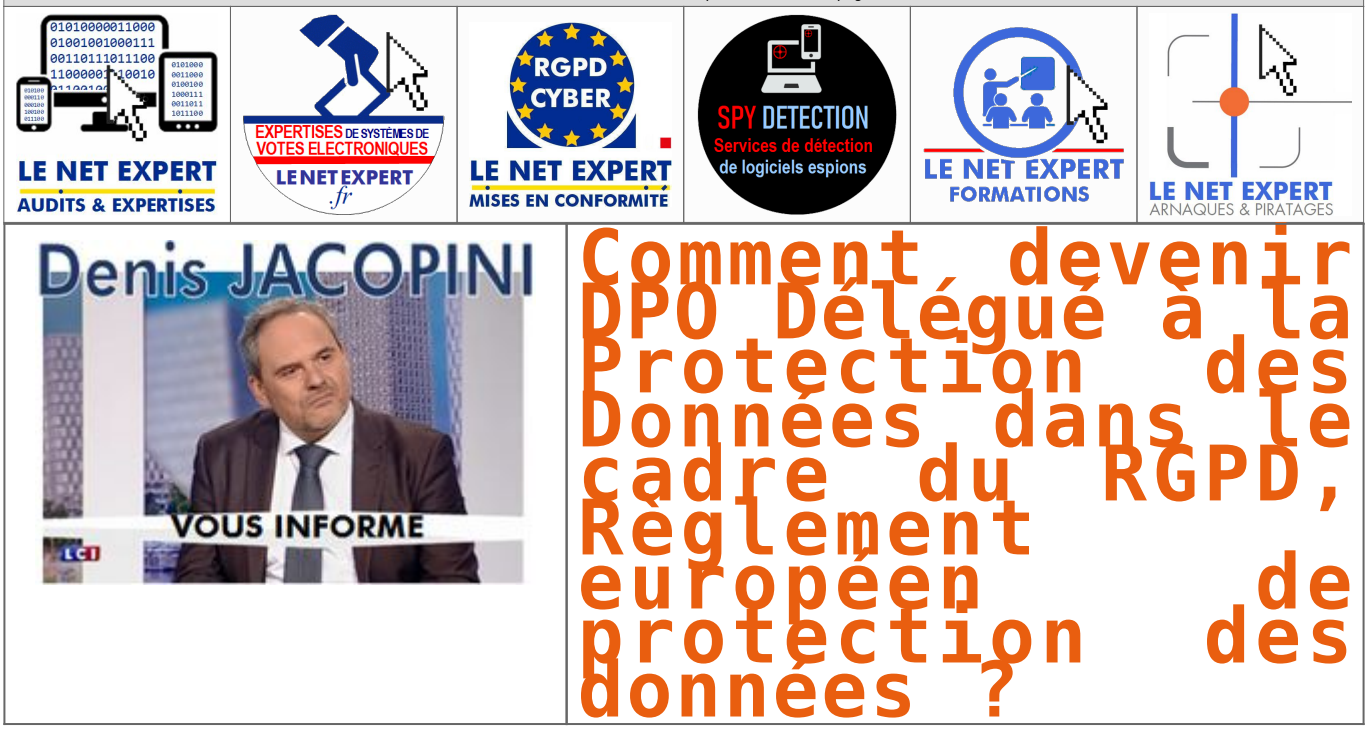
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

# Comment devenir DPO Délégué à la Protection des Données dans le cadre du RGPD, Règlement européen de protection des données ?

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



**Entré en vigueur en mai dernier, le Règlement général sur la protection des données impose de nouvelles règles en matière de gestion des données personnelles. Avec l'obligation pour les entreprises de se mettre en conformité avant mai 2018. Ce qui implique une modification des contrats fournisseurs.**

**Qui est concerné?**

Le RGPD s'applique « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. »

Ce règlement s'applique à toute structure (responsable de traitement des données ou sous-traitant) ayant un établissement dans l'Union européenne ou bien proposant une offre de biens ou de services visant les personnes qui se trouvent sur le territoire de l'Union européenne.

Les actions de profilage visant cette cible sont également concernées. Ainsi, alors que la loi Informatique et libertés se basait sur des critères d'établissement et de moyens de traitement, le règlement européen 16-679 introduit la notion de ciblage: le critère principal d'application est désormais le traitement des données d'une personne se trouvant au sein de l'UE.

**Qu'est-ce qu'une donnée à caractère personnel?**

L'une des difficultés posées par le RGPD va consister à définir les données personnelles concernées. Le règlement stipule qu'il s'agit de « toute information concernant une personne physique identifiée ou identifiable », directement ou indirectement.

Des données indirectement identifiantes, telles qu'un numéro de téléphone, ou un identifiant, sont donc concernées. De même, les données comportementales collectées sur Internet (notamment recueillies dans le cadre d'actions marketing de profilage), si elles sont corrélées à une identité, deviennent des données à caractère personnel.

Selon le traitement appliqué aux données, des informations non identifiantes peuvent ainsi devenir identifiantes, par croisement des informations collectées.

**Quelles obligations pour les entreprises?**

La loi Informatique et libertés se basait sur du déclaratif initial et des contrôles ponctuels. Le nouveau règlement européen remplace cette obligation de déclaration par une obligation de prouver à chaque moment que l'entreprise protège les données. Dès lors, la structuration même des outils permettant la collecte des données (CRM, DMP, solutions de tracking ou de géolocalisation…), mais aussi les contrats passés avec les fournisseurs et clients sont impactés (voir encadré ci-dessous).

« Le règlement couple des notions techniques et juridiques », souligne Thomas Beaugrand, avocat au sein du cabinet Staub & Associés. Il introduit des nouveaux principes et concepts qui renvoient désormais vers plus de précautions techniques. Par ailleurs, les entreprises ont, entre autres, l'obligation de donner la finalité précise de la collecte des données (il s'agit du principe de minimisation, un des grands principes de la dataprotection, qui impose que seules les données nécessaires à la finalité poursuivie pourront être collectées).

Le GRPD impose également le principe de conservation limitée des données, ainsi que celui de coresponsabilité des sous-traitants et des entreprises en matière de protection de la data, qui permet de distribuer les responsabilité en fonction de la mainmise de chacun sur les données. Cette notion de coresponsabilité doit être intégrée dès maintenant dans les contrats passés avec les fournisseurs: en effet, le sous-traitant désigné par une organisation pour assurer le traitement des données devient, avec le RGPD, coresponsable de la légalité des traitements. Il sera donc tenu d'informer ses clients et de tenir des registres pour recenser les données, ainsi que d'accepter les audits demandés par son client pour s'assurer de la conformité des traitements.

Les sous-traitants concernés peuvent être, par exemple, l'éditeur d'un CRM en ligne, le routeur d'une campagne d'e-mailing, un service de relation client, etc. Le responsable du traitement, de son côté, doit s'assurer que ses fournisseurs ont pris les mesures nécessaires pour assurer la sécurité des données.

Enfin, parmi les changements majeurs, la nomination d'un DPO, ou délégué à la protection des données, qui sera obligatoire dans tout le secteur public, ainsi que dans les structures privées qui font des traitements de données exigeant un suivi régulier et systématique des personnes à grande échelle (dans le secteur du marketing, notamment). Il sera le garant de la conformité au règlement. Quel impact sur les contrats fournisseurs? Pour se mettre en conformité avec le RGPD, les directeurs achats devront veiller à renforcer les contrats passés avec leur fournisseurs…

**Le délégué à la protection des données**

Le règlement européen consacre la fonction de Délégué à la Protection des Données (DPD ou en anglais DPO) dans les organismes.

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un DPO :

1. s'ils appartiennent au secteur public,
2. si leur activité principale les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
3. si leur activité principale les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations.

**Les responsables de traitement peuvent opter pour un DPO mutualisé ou externe.**

Véritable « chef d'orchestre » de la conformité en matière de protection des données, le DPO est chargé :

1. d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
2. de contrôler le respect du règlement et du droit national en matière de protection des données ;
3. de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA ou EIVP) et d'en vérifier l'exécution ;
4. de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

**QUI PEUT ÊTRE DPO ?**

Le DPO est désigné sur la base de son expertise.

**CONSEILS POUR LA MISE EN PLACE DU FUTUR DPO**

Compte tenu que jusqu'au 25 mai 2018, ne non respect de la Loi Informatique et Libertés est passible de 5 ans de Prison et jusqu'à 300 000 euros d'amende, nous vous conseillons fortement d'entamer au plus vite les démarches suivantes déclarer un CIL avant le 25 mai 2018 ou désigner un DPO après. Puis :

1. Réaliser ou faire réaliser un indispensable état des lieux (appelé aussi audit) afin d'identifier l'ensemble des traitements de données personnelles et l'ensemble des lieux dans lesquels des données personnelles sont traitées ;
2. Identifier dans la Loi Informatique et Libertés ou dans le RGPD des particularités propres à votre métier qui vous autorise à certains traitements interdits à d'autres activités ou qui nécessiteraient une demande d'autorisation ;
3. Faire une analyse de risque autour des traitements et des données personnelles présentes dans votre établissement.  Cette étape indispensable peut être assurée par notre Expert Denis JACOPINI, Certifié ISO 27005 Risk Manager ;
4. Porter au registre l'ensemble des traitements identifiés ;
5. Mettre en conformité les traitements qui ne respectent pas la loi ou le règlement.
6. Suivre régulièrement l'évolution des traitements au sein de l'organisme.

**Articles du règlement associés**

Article 13 | Article 14 | Article 30 | Article 33 | Article 35 | Article 36 | Article 37 | Article 38 | Article 39 | Article 47 | Article 57

**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

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 :

Nous animons des Formations sur le RGPD en individuel ou en groupes

Nous vous accompagnons dans la mise en conformité RGPD de votre établissement

**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"]

---

Original de l’article mis en page : Le règlement européen de protection des données et les contrats fournisseurs

---

# Google sommé de livrer des mails stockés à l’étranger


Google sommé de livrer des mails stockés à l’étranger

---

**Contredisant une jurisprudence Microsoft, un juge a ordonné à Google de livrer les mails stockés sur des serveurs en dehors des Etats-Unis. La firme a fait appel.**


Décidément la jurisprudence américaine sur l'extraterritorialité des mandats de perquisitions sur les données conservées hors des Etats-Unis joue à la girouette. A la fin janvier, Microsoft gagnait une seconde victoire sur ce sujet. Les juges de la Cour d'Appel de New York ont jugé, dans la douleur, que le Secure Communications Act (SCA) sur lequel se base les mandats n'avait pas en 1986 était conçu pour des données localisées hors du territoire américain.

Une jurisprudence mise à mal par une autre affaire concernant Google. Ce dernier a été sollicité par le FBI dans une affaire de fraude datant du 2 août 2016 et une autre du 19 août portant sur un vol de données industrielles sur le territoire américain. Mais certaines données des comptes des suspects étaient disséminées sur des datacenters de Google à l'étranger. La firme américaine a expliqué que pour des raisons de performances, les courriers électroniques pouvaient être découpés en petits morceaux et stockés sur différents serveurs à l'étranger. La firme de Mountain View s'appuyait donc sur les décisions favorables à Microsoft en matière de non extra-territorialité des mandats de perquisition pour refuser le mandat du FBI.

## Une violation de la vie privée aux États-Unis

Mais le juge, Thomas Rueter, du tribunal de Philadelphie, en a décidé autrement. Il considère en effet que « *le fait de transférer électroniquement des données d'un serveur dans un pays étranger vers le datacenter de Google en Californie ne constitue pas une saisie* ». Cette notion de saisie est définie par le 4ème amendement de la Constitution américaine qui stipule, « *le droit des citoyens d'être garanti dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir* ».
La qualification de saisie n'est pas retenue par le juge, car « *il n'y a aucune interférence significative avec l'intérêt possessif du titulaire du compte dans les données utilisateur* ». Il poursuit en expliquant que Google transfère régulièrement des données entre ses installations sans que les utilisateurs en soient mis au courant et cela ne les empêche pas d'accéder à leur données, ni ne remet en question leur droit de propriété. Et si interférence il y a, elle est « *minime et temporaire* ».
Pour motiver sa décision, le juge Rueter, précise que « *même si la récupération des données électroniques par Google depuis ses multiples centres de données à l'étranger a le potentiel d'une invasion de la vie privée, la violation réelle de la vie privée se produit au moment de la divulgation aux États-Unis* ». Pour lui, la perquisition et la saisie ont eu lieu aux Etats-Unis et non à l'étranger, le mandat de perquisition est alors contraignant pour Google. Ce dernier a déjà annoncé sa décision de faire appel de ce jugement.

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits 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.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

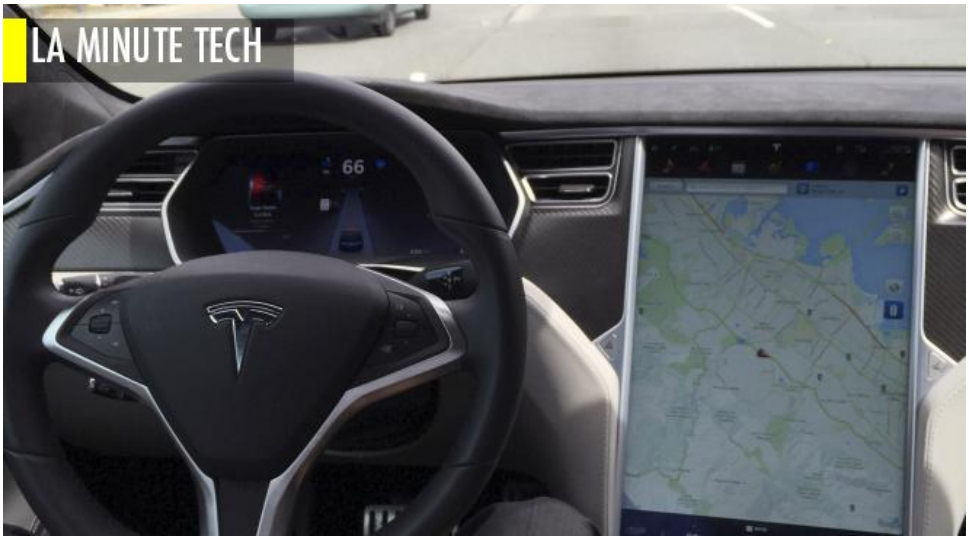
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

# Original de l'article mis en page : Google sommé de livrer des mails stockés à l'étranger

# Apprenez à vous protéger contre le piratage de vos objets connectés du quotidien




Apprenez à vous protéger contre le piratage de vos objets connectés du quotidien

**Souhaitant mettre rapidement sur le marché leurs produits, les fabricants d'objets connectés ont eu tendance à négliger l'aspect sécurité, contribuant ainsi à la vulnérabilité de leurs utilisateurs face à de possibles attaques.**

**Atlantico : En septembre et octobre 2016, deux attaques DDOS ont été particulièrement marquantes : la première sur l'entreprise OVH et la deuxième sur DYN. Dans les deux cas, ces attaques ont été rendues possibles par les objets connectés. Malgré l'ampleur de ces attaques, celles-ci sont à relativiser. Dans une récente étude réalisée pour le compte de l'entreprise HSB, on note que seulement 10% des utilisateurs ont été touchés par des problèmes de piratage. Quels sont les risques du piratage des objets connectés ?**

## Quel peut être le préjudice porté aux particuliers et aux entreprises ?

**Yvon Moysan :** Une attaque DDoS ou attaque par déni de service massive vise à **rendre un serveur, un service ou une infrastructure indisponibles en surchargeant la bande passante du serveur, ou en accaparant ses ressources jusqu'à épuisement.** Lors d'une attaque DDoS, une multitude de requêtes sont envoyées simultanément et depuis de multiples endroits. L'intensité de ce « tir croisé » rend le service instable, voire indisponible. **Le risque d'être confronté à ce type d'attaque est important et surtout les tentatives sont nombreuses**. Dans le cas de la société américaine Dyn que vous évoquez, celle-ci a été victime d'une attaque de plus d'un Téra-octet par seconde, ce qui pourrait concerner environ 10 millions d'objets connectés piratés. Ce niveau d'intensité est toutefois très rare.

**Le préjudice subi dépend du type d'objets connectés piratés et du caractère sensible des données des particuliers.** Si la majorité des objets connectés contiennent rarement des informations aussi sensibles que celles qui sont stockées sur un ordinateur, **il en existe des sensibles comme les voitures connectées ou les fusils intelligents qui, piratés à distance, peuvent représenter un véritable danger, potentiellement mortel pour l'utilisateur.** Et **ce risque s'est d'ores et déjà avéré.** Des experts en sécurité informatique ont ainsi réussi à prendre le contrôle à distance d'une Jeep Cherokee. Ils ont pu agir sur la vitesse, freinant et accélérant à leur guise, envoyant même la voiture dans le fossé alors que pour le fusil intelligent, d'autres experts ont réussi a bloqué le déclenchement du tir.

**Le risque existe également pour des objets plus communs comme les applications de smart home.** Des hackers ont ainsi réussi à bloquer la température de thermostats connectés à une température polaire ou saharienne. Plus préjudiciable, des hackers ont pris le contrôle de caméras de surveillance, récupéré les vidéos enregistrées, et au final les ont diffusées sur le Web. Un baby phone a également été la cible d'un hacker terrorisant un bébé et ses parents. En prenant le contrôle de l'appareil équipé d'une caméra, d'un micro et d'un haut-parleur, celui-ci s'est mis à hurler des insanités sur le nourrisson. **Le risque peut surtout être généralisé si des hackers réussissent à prendre le contrôle des réseaux d'électricité ou de gaz sur un quartier par exemple.** Il devient en effet possible de plonger toute une zone dans le noir ou, en fonction des données récoltées sur la consommation, de savoir quelles habitations sont occupées ou pas, en vue d'éventuels cambriolages.

Cela peut ensuite être contraignant pour la société qui a fabriqué et vendu les objets piratés car cela révèle **la faiblesse du niveau de sécurité**. Dans le cas de l'attaque de la société Dyn, une partie des objets connectés étaient ceux de la société chinoise Xiongmai, qui a dû les rappeler en urgence pour leur appliquer un correctif de sécurité. Cela peut aussi être problématique pour les clients de la société victimes de l'attaque. Dans le cas de Dyn, cela a eu pour conséquence de rendre inaccessible pendant une dizaine d'heures des sites comme Twitter, Ebay, Netflix, GitHub ou encore PayPal.

## On peut aussi s'interroger sur certaines pratiques des constructeurs. Le fait de mettre un mot de passe commun à tous les appareils avant une première connexion a déjà été pointé du doigt. Quels autres dysfonctionnements peut-on mettre en avant ? Face à l'augmentation du nombre d'objets connectés, comment s'adaptent précisément les constructeurs en termes de sécurité ?

Tout d'abord il est important de préciser que ce type d'attaques par déni de service n'a rien de nouveau : les cybercriminels utilisent depuis des années des armées d'ordinateurs piratés pour inonder de requêtes les sites ciblés et les rendre inaccessibles.

La nouveauté réside ici dans le nombre croissant des objets connectés qui accroit de manière exponentielle les possibilités d'attaques. Or **la puissance d'une attaque dépend essentiellement du nombre de périphériques piratés, d'où l'intérêt de passer par les objets connectés**. Il existe en effet **plusieurs milliards d'objets connectés dans le monde contre quelques centaines de millions d'ordinateurs.** Pour y faire face, il existe des solutions proposées par les hébergeurs pour protéger leurs serveurs des attaques. Ces solutions permettent, par exemple, d'analyser en temps réel et à haute vitesse tous les paquets, et si besoin d'aspirer le trafic entrant, voire de mitiger, c'est-à-dire repérer tous les paquets IP non légitimes, tout en laissant passer les paquets IP légitimes.

Du côté des constructeurs d'objets connectés, tous les thermostats, toutes les webcams ou les imprimantes ne présentent pas de faille de sécurité, mais il s'agit d'un point préoccupant car **pour la plupart des fabricants, la sécurité n'a pas été la priorité dès le départ**, **ayant souvent été donnée à la rapidité de la mise à disposition du produit sur le marché pour répondre à un nouveau besoin**. Il faudrait que des normes minimales de sécurité puissent être définies comme le cryptage des données échangées sur le réseau ou l'exigence de mot de passe sécurisé mêlant caractères spéciaux et chiffres pour l'accès à distance et l'interdiction de mots de passe comme « 123456 » particulièrement vulnérables. Dans cet esprit, la Online Trust Alliance, qui regroupe des éditeurs comme Microsoft, Symantec (Norton) et AVG, a rédigé un guide des bonnes pratiques pour minimiser les risques de piratage. Les constructeurs d'objets connectés peuvent, par ailleurs, faire évaluer leurs systèmes de cryptage par des sociétés spécialisées, pour identifier les éventuelles vulnérabilités.

## Comment se prémunir du piratage d'objets connectés ? Quels sont les bons comportements à adopter ? Que faire en cas de doute ?

**Du côté des particuliers, il apparait préférable de privilégier les produits de sociétés à la pointe des questions de sécurité informatique, comme Google ou Apple.** Il faut également installer régulièrement **les mises à jour de sécurité et les mises à jour logicielles**, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut **changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle.** Pour finir, il faut **limiter l'accès d'un objet connecté aux autres objets connectés dans la maison.** Par exemple, si vous avez une Smart TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau. Par exemple, il n'est pas vraiment nécessaire que l'imprimante soit connectée à la télévision.

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits 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.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

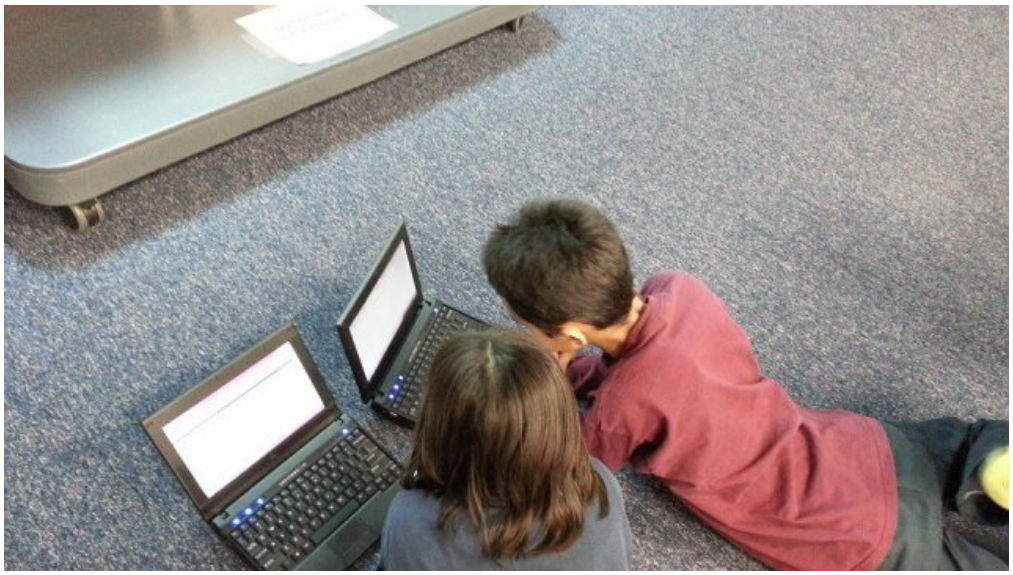
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Attention danger : apprenez à vous protéger contre le piratage de vos objets connectés du quotidien | Atlantico.fr

---

# Comment rendre Internet plus sûr pour les jeunes ?



Comment rendre Internet plus sûr pour les jeunes ?

---

**PartagerTwitterPartagerEnvoyer »Le Safer Internet Day est un événement mondial annuel organisé par le réseau européen Insafe, en février, pour promouvoir un Internet meilleur auprès des jeunes, de leurs parents et de la communauté éducative. »**

# Pour un internet plus sûr

Cette année, le **Safer Internet Day aura lieu le 7 février 2017** et se poursuivra tout au long du mois. L'objectif est de multiplier l'organisation – par les enseignants, les éducateurs, les associations de parents – d'actions de **sensibilisation sur la citoyenneté numérique** et le cyberharcèlement.

« Les cyberviolences et, plus spécifiquement, le **cyberharcèlement, sont parmi les risques les plus importants** auxquels peuvent être confrontés les jeunes internautes aujourd'hui. Alors que l'utilisation des réseaux sociaux explose, l'accent doit être mis sur la compréhension des enjeux de l'Internet, du fonctionnement de ces réseaux et de l'importance des données. »

**Internet Sans Crainte** est un « programme national de sensibilisation des jeunes aux enjeux de l'Internet.. Opéré par Tralalere depuis 2007, il est placé sous l'égide de l'Agence du numérique. Il fournit aux acteurs éducatifs les outils pour agir auprès du jeune public : comprendre ce qu'est Internet, **comment garder sa vie privée… privée, comment sécuriser ses recherches sur la toile,** comment se défendre en cas de cyber harcèlement…

Exemples d'actions qui vont être menées en BFC : du bon usage d'internet, le 14 février, à l'accueil periscolaire d'Esprels (70), internet sans crainte à Autun (71)  le 14 mars, le Safe internet day le 7 février à Chaussin (39).

**Les explications de Philippe Cayol**, responsable du programme Internet Sans Crainte.

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits 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.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : France 3 Bourgogne-Franche-Comté – Comment rendre Internet plus sûr pour les jeunes… tout un programme à découvrir à 9H50 le matin

---

# Protéger son identité contre le vol sur Internet devrait être une priorité

Protéger son identité contre le vol sur Internet devrait être une priorité

---

**Selon une étude concernant le vol d'identité et menée aux États-Unis par l'entreprise spécialisée dans la cybersécurité mobile Lookout auprès de 2000 clients, les délits concernant les données personnelles sont en pleine expansion. Ils constituent l'un des principaux soucis des usagers d'Internet et de la téléphonie mobile, qu'ils soient particuliers ou entreprises. Actuellement, le vol… Lire la suite**

Actuellement, le vol d'identité est considéré comme un phénomène inéluctable d'après les enquêtes réalisées par Lookout. Les résultats démontrent que près de 35 % des sondées ont été victimes de vol d'identité. 41 % affirment que leurs données personnelles ne peuvent plus être sécurisées et, à un moment donné, elles seront inévitablement volées. D'ailleurs, aux États-Unis, le pourcentage d'infraction sur les identités des personnes a augmenté de près de 20 % depuis octobre 2015.

## Internet : principal moyen de vol

Lookout affirme que le vol de données personnelles ne se passe plus par les méthodes classiques telles que la fouille des ordures dans les rues ou encore le vol de courrier dans les boîtes aux lettres ou il est très facile d'y trouver des informations permettant d'accéder aux numéros de carte de crédit ou de comptes divers. De nos jours, les criminels sont plus malins et bien plus discrets en usant de moyens sophistiqués et d'Internet comme les techniques de « phishing ».

Cette méthode profite de la faille humaine et non de l'informatique. Les voleurs se font passer pour une banque, un opérateur téléphonique ou une entreprise pour pousser la victime à se connecter sur leur site à travers un faux lien hypertexte. De cette manière, ils peuvent récolter des informations personnelles (des coordonnées bancaires surtout) qu'ils vont utiliser pour réaliser des achats ou des transferts d'argent vers leur compte.

En effet, l'étude menée par Lookout démontre que 60 % des Américains ont effectué à leur insu, des achats à de grandes entreprises de vente en ligne ou des transactions bancaires à cause d'une cyberattaque via de courriels frauduleux d'hameçonnage (phishing).

## Les chiffres démontrés par l'étude de Lookout

D'autres chiffres révèlent aussi que les personnes ne se sentent pas en sécurité : 77 % craignent de perdre leur numéro de sécurité sociale, 74 % leurs données bancaires, 71 % leur code et carte de crédit et 56 % leurs données personnelles.

Par ailleurs, la plus grande peur des gens concerne le fait qu'ils ne soient pas immédiatement au courant du vol de leur identité au moment des actes de fraudes commises par les criminels. Selon l'enquête faite par Lookout, une personne victime d'un vol d'identité ne le découvrira que par une lettre postale (33 %), une information télévisée ou radio (31 %) ou un mail inattendu (31 %). Cela résulte du fait que les factures sur les crimes commis lui sont toujours renvoyées plus tard par mail ou par la poste.

Toujours d'après l'étude, 65 % des personnes ayant subi un vol ou une usurpation de leur identité via un site sur lequel elles se sont inscrites n'en seront averties qu'un mois après la cyberattaque. De même, 75 % des usurpés ne connaissent pas les actions à entreprendre dans de telles situations.

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits 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.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Le vol d’identité en nette progression : les données personnelles ne sont plus sécurisées