Protection des données : ce qui va changer pour les entreprises en 2018

Protection des données : ce qui va changer pour les entreprises en 2018

En mai 2018, un règlement européen va entraîner d'importants changements dans la pratique des entreprises en matière de gestion des données personnelles. En quoi consistent ces changements et comment s'y préparer ?

Protection des données : ce que prévoit le règlement européen de 2016

Contrairement à une directive, le règlement européen, adopté en 2016, est directement applicable dans l'ensemble de l'Union européenne sans nécessiter de transposition dans les différents Etats membres et ce à partir du 25 mai 2018. Il concerne toutes les entreprises utilisant des données personnelles.
Ainsi, à cette date, les responsables de traitement devront s'être mis en conformité avec le règlement sous peine de sanctions.

Principal changement :
Ce règlement marque le passage d'une logique de « formalités préalables » (déclarations, autorisations) à une logique de « conformité » dont les acteurs seront responsables sous le contrôle du régulateur (la CNIL en France). Ainsi, les responsables de traitements de données n'auront plus à effectuer de déclarations à la CNIL dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes.
Par contre, ils devront d'entrée mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles. Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »). Ils devront également être capables de démontrer cette conformité à tout moment.

	Pour les traitements à risque, il faudra toutefois conduire une étude d'impact complète faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Cela concerne notamment les données sensibles qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi les données génétiques ou biométriques. En cas de risque élevé, il faudra consulter la CNIL avant de mettre en œuvre ce traitement, cette dernière pouvant décider de s'y opposer.

Ce règlement renforce par ailleurs les droits des personnes. En effet, chaque personne concernée par les traitements de données va avoir le droit à la mise à disposition d'une information claire, intelligible et aisément accessible et va devoir donner son accord pour le traitement des données. La preuve de ce consentement incombant au responsable de traitement.

Protection des données : mise en place des délégués à la protection des données

Le règlement européen instaure des délégués à la protection des données (DPD). Ce seront les successeurs des correspondants informatique et libertés (CIL) dont plus de 17 700 organismes sont d'ores et déjà dotés en France et dont la mise en place permet de se dispenser de certaines déclarations.
A la différence du CIL, dont la désignation est actuellement optionnelle, la désignation du DPD est obligatoire dans le secteur public et pour les responsables de traitement et les sous-traitants dont les activités principales les amènent :
• à réaliser un suivi régulier et systématique des personnes à grande échelle ;
• à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions.
Pour les autres, leur désignation est facultative…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Protection des données : ce qui va changer pour les entreprises – Editions Tissot*

Le Bitcoin n’es t pas la seule monnaie virtuelle

Le Bitcoin n’est pas la seule monnaie virtuelle

La plus connue des crypto-monnaies, le Bitcoin, est valorisée en bourse à 19,4 milliards de dollars. Ces monnaies électroniques n'ont plus rien de virtuelles. Classement.

Coinmarketcap.com a réalisé le classement des crypto-monnaies en fonction de leur valorisation boursière. Sans surprise, le Bitcoin arrive en tête avec une capitalisation boursière de 19,4 milliards de dollars en avril. Viennent ensuite l'Etherum, une chaîne de bloc lancée en 2015 qui utilise l'Ether comme moyen de paiement, valorisée à 3,9 milliards de dollars. Puis, le Ripple à 1,2 milliard de dollars. Pour se différencier du Bitcoin, nombre d'autres monnaies cryptographiques mettent en avant un anonymat total, là où il n'est que partiel chez Bitcoin.

1. Bitcoin
Lancement : 2009
Capitalisation boursière au 10 avril 2017 : 19,4 milliards de dollars
Fonctionnement du Bitcoin : transfert d'argent entre personnes sur internet.

2. Ethereum
Lancement : 2015
Capitalisation boursière en avril 2017 : 3,9 milliards de dollars
Fonctionnement : l'Ethereum est le protocole d'échange décentralisé, l'Ether est son unité de compte et moyen de paiement.

3. Ripple
Lancement : 2012
Capitalisation boursière en avril 2017 : 1,2 milliard de dollars
Fonctionnement de Ripple : à la fois système de règlement brut réel, marché des changes et réseau d'envois de fonds.

4. Litecoin
Lancement : 2011
Capitalisation boursière en avril 2017 : 449, 8 millions de dollars
Fonctionnement : comme Bitcoin, elle fonctionne sous licence libre, le code du Litecoin est une modification du code Bitcoin.

5. Dash
Lancement : 2014
Capitalisation boursière en avril 2017 : 443,6 millions de dollars
Fonctionnement : mot valise de digital et cash. Ex Darkoin, elle veut s'affranchir des limitations du Bitcoin et promet l'anonymat.

6. Monero
Lancement : 2014
Capitalisation boursière en avril 2017 : 304,5 millions de dollars
Fonctionnement : se dit totalement anonyme, contrairement aux autres crypto-monnaies qui sont des clones de Bitcoin, Monero repose sur un fonctionnement cryptographique différent, et utilise des signatures en cercle. Un utilisateur ne peut connaître le contenu ni l'historique des transactions.

7. Ethereum Classic
Capitalisation boursière en avril 2017 : 234 millions de dollars
Fonctionnement : à la différence de l'Ethereum, l'Ethereum classic est "unstoppable".

8. NEM
Lancement : 2015
Capitalisation boursière en avril 2017 : 186,6 millions de dollars
Fonctionnement : Nem pour New Economic Movement. Sa monnaie est le Xem. Nem réécrit le code de zéro.

9. Augur
Capitalisation boursière en avril 2017 : 104 millions de dollars

10. MadeSafeCoin
Capitalisation boursière en avril 2017 : 88, 5 millions de dollars

[Plus d'infos sur l'article de Forbes]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Bitcoin, Ethereum, Ripple, classement des crypto-monnaies dans le monde*

Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »

Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »

Ce texte entre en vigueur le 1er avril 2017. Par application de la loi de modernisation de notre système de santé, il « décrit les modalités de gouvernance et de fonctionnement du système national des données de santé (SNDS) qui a vocation à regrouper les données de santé de l'assurance maladie obligatoire, des établissements de santé, les causes médicales de décès, les données issues des Maisons départementales des personnes handicapées ainsi qu'un échantillon de données de remboursement d'assurance maladie complémentaire ».

« Il fixe en outre la liste des organismes, établissements et services bénéficiant d'accès permanents aux données du SNDS en raison de leurs missions de service public ainsi que les modalités de ces accès. Ce texte prévoit également des possibilités d'accès ponctuel aux données du SNDS. Enfin, il prévoit l'information des personnes auxquelles les données se rapportent, et leurs droits d'accès, de rectification et d'opposition qui s'exercent auprès de la caisse d'assurance maladie dont dépend la personne ».

Consulter

• Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »
• Délibération n° 2016-316 du 13 octobre 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé (demande d'avis n° 16018114)

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé » – APHP DAJ*

Windows 10 : Microsoft dévoile les données personnelles qu'il récolte

Microsoft dévoile les données personnelles que Windows 10 récolte

---

Un cadre haut placé chez Microsoft vient de révéler la publication d'une liste des données personnelles que l'entreprise récolte sur Windows 10. Si Microsoft tente de rassurer sur sa politique de confidentialité et la sécurisation des données, ce nouveau procédé est susceptible de relancer des débats.

Selon le site theverge.com, le chef Windows Terry Myerson explique que **Microsoft publie désormais des informations sur les données collectées** dans le cadre de Windows 10. Ces données sont publiées sur le site TechNet de Microsoft. Dans le cadre de la dernière mise à jour Creators Update et de la nouvelle politique de confidentialité, les contrôles autour des niveaux de collecte sont renforcés.

Les données personnelles : une question de sécurité des utilisateurs

Si Microsoft tente de rassurer sur les contrôles et la sécurisation des données personnelles, il n'en demeure pas moins que ses pratiques posent problème. **Microsoft est soupçonné de suivre ses utilisateurs via des traçeurs** et de ne pas respecter des choix de confidentialité exprimés par les utilisateurs Windows 10. Il y aurait danger pour le droit au respect de la vie privée. Il peut même s'agir d'espionnage.
Toutefois, les autorités de régulation veillent au grain. La France vient d'ordonner à Microsoft de cesser toute traçabilité. L'agence de protection des données de l'Union Européenne ont mis en garde contre les insuffisances des changements apportés par Microsoft Creators Update.

Le débat sur les données personnelles relancé ?

La révélation des données peut constituer une **atteinte du droit à la protection de la vie privée.** Il est tout de même légitime de se poser la question de savoir si les autorités de régulation ne protège pas certains intérêts particuliers ou si leur examen n'est pas dicté par un esprit partisan.
Après tout, Amazon, Facebook et Google sont déjà capables de repérer vos habitudes de consommation, et de vous proposer des produits en lien avec vos acquisitions passées. Même si Google a déjà pu faire l'objet d'une procédure à l'initiative de l'UE, on peut se demander pour quelles raisons, des entreprises comme Amazon, ne pourraient pas subir le même traitement que celui réservé à Google et Microsoft…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Windows 10 : Microsoft dévoile les données personnelles qu'il récolte*

Voyagez aux Etats-Unis et laissez vos données être espionnées

Voyagez aux Etats-Unis et laissez vos données être espionnées

---

L'administration Trump envisage de demander aux voyageurs arrivant aux Etats-Unis l'accès aux données de leur smartphone et à leurs comptes Twitter, Facebook ou LinkedIn. Une sévère menace pour la cybersécurité des entreprises européennes.

Cette fois-ci, la côte d'alerte est clairement franchie. Dans ses colonnes, le *Wall Street Journal* évoque un projet de l'administration Trump qui pourrait forcer les visiteurs arrivant aux Etats-Unis à communiquer aux autorités les contacts et contenus présents sur leur téléphone mobile ainsi que les mots de passe de leurs comptes de réseaux sociaux, permettant d'accéder aux messages privés envoyés sur ces canaux. Un projet qui ne serait pas limité aux pays soumis aux règles de sécurité les plus strictes – et dont les ressortissants doivent obtenir un visa -, mais concernerait aussi les pays considérés comme des alliés des États-Unis, dont la France.
Rappelons que, pour se rendre de façon temporaire sur le sol américain, pour affaires ou en tant que touriste, les Français doivent déjà solliciter une autorisation électronique (Esta), valable 2 ans. En février, le ministre de l'Intérieur américain (Homeland Security) avait déjà évoqué, lors d'une audition devant le Sénat, le fait que les voyageurs étrangers (notamment issus des 6 pays blacklistés par un décret de l'administration Trump) venant aux États-Unis seraient tenus de fournir leurs mots de passe sur les médias sociaux aux autorités d'immigration avant de rentrer sur le territoire américain.

La peur de l'espionnage économique

Selon le *Wall Street Journal,* cette mesure serait donc étendue à d'autres pays et aussi aux contacts téléphoniques. « *S'il existe un doute sur les intentions d'une personne venant aux États-Unis, elle devrait avoir à prouver la légitimité de ses motivations, vraiment et véritablement jusqu'à ce que cela nous satisfasse* », a expliqué le conseiller principal du Homeland Security, Gene Hamilton, cité par le quotidien économique.
Si la question ne manquera pas de soulever de vifs débats sur le sol américain et entre les États-Unis et ses partenaires et si une procédure de la sorte pose également quelques questions pratiques assez épineuses, la perspective risque d'échauder de nombreuses entreprises européennes. Car, les activités des services de renseignement US associent sans vergogne antiterrorisme et espionnage économique au profit des entreprises américaines. Une porosité d'ailleurs assumée, comme l'ont montré de nombreux documents dévoilés par Edward Snowden ou *Wikileaks* et révélant les activités de la NSA en matière d'espionnage économique. Les activités de cette nature ne sont d'ailleurs pas limitées à la seule agence de Fort Meade, mais s'étendent à toute la communauté du renseignement aux Etats-Unis.
Au passage, les mesures envisagées par l'administration Trump signeraient probablement l'arrêt de mort du Privacy Shield, l'accord transatlantique sur les transferts de données qui succède au Safe Harbor. Pour mémoire, ce dernier érige comme credo le fait que les données des citoyens européens exportées aux Etats-Unis bénéficient de la même protection que celle que leur accorde le droit européen. En février, les CNIL européennes s'étaient déjà inquiétées des conséquences possibles du décret sur l'immigration du Président Trump sur cet accord…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation 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

Source : *L'entrée aux Etats-Unis conditionnée par les données des smartphones ?*

Limiter les risques venant des drones en les immatriculant. Une bonne idée ?

Limiter les risques venant des drones en les immatriculant. Une bonne idée ?

Hostile à une surveillance en réseau, le fabricant DJI propose une immatriculation électronique que seules les forces de l'ordre pourraient exploiter.
Jean-Michel Normand

L'idée trotte dans la tête de nombre de législateurs. Installer à bord des drones de loisir un système de reconnaissance électronique fait déjà partie de l'arsenal législatif adopté l'an passé par les parlementaires français, sans pour autant que des précisions techniques aient été définies. L'Italie et le Danemark ou la FAA, l'Aviation civile américaine, l'ont également inscrit à leur programme. Dans une proposition qu'il vient de rendre publique, le fabricant de drones chinois DJI préconise une identification électronique *« simple, qui maintient un équilibre entre le respect de la vie privée de l'opérateur du drone et les légitimes préoccupations des autorités relatives à l'utilisation »* de ces appareils.

1.
Plusieurs pays, dont la France, envisagent d'imposer une signature électronique. NIR ELIAS / REUTERS

« Comparable à une plaque d'immatriculation automobile »
DJI est favorable à ce que tous les drones commercialisés soient capables d'émettre un signal qui indique leur localisation, mais aussi un code d'identification *« comparable à une plaque d'immatriculation automobile »* en mode électronique. Ce code serait émis sur les bandes de fréquence (2,4 GHz et 5,8 GHz) utilisées pour la liaison entre le drone et la radiocommande du pilote et pour la liaison vidéo. Il suffirait de réaliser une mise à jour des protocoles de contrôles radio existants. L'information pourrait être captée par la police ou un particulier furieux de voir un quadricoptère évoluer au-dessus de sa propriété, à condition qu'il soit équipé d'un récepteur adapté. Il lui faudra alors se tourner vers les forces de l'ordre, seules autorisées (avec les autorités aéroportuaires, notamment) à remonter jusqu'au titulaire de l'immatriculation électronique…[lire la suite]

Commentaire de Denis JACOPINI :
Je trouve personnellement l'idée intéressante, encore faut-il que :
1. L'émission de cette information ne puisse pas être perturbée (j'en doute) ;
2. L'émission du code du drone ne puisse pas être modifiée (plus facile) ;
3. Cette procédure soit légiférée et suivie par tous les constructeurs mondiaux.

Ceci n'empêchera pas les groupes les plus obscurs d'utiliser des drones volés non pourvus de cette signature.
À mon avis, la mise en place de ces précautions ne concernent que l'utilisateur lambda, pas ceux que l'on craint actuellement le plus sur le territoire.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Comment immatriculer les drones de loisir*

Secret des correspondances : Ce que change la Loi Lemaire à partir de 2017

Secret des correspondances : Ce que change la Loi Lemaire à partir de 2017

Le 30 mars 2017 a été publié au Journal Officiel un décret d'application de la loi pour une République numérique relatif au secret des correspondances (article 68 de la loi). A cette occasion, la CNIL en profite pour faire le point sur cette notion et sur ce qui change pour les utilisateurs de services de messagerie électronique.

Le 30 mars 2017 a été publié au Journal Officiel un décret d'application de la loi pour une République numérique relatif au secret des correspondances (article 68 de la loi). A cette occasion, la CNIL en profite pour faire le point sur cette notion et sur ce qui change pour les utilisateurs de services de messagerie électronique.

La correspondance privée se définie comme tout message exclusivement destiné à une ou plusieurs personnes physiques ou morales, déterminées et individualisées. L'exemple le plus concret est le courriel échangé entre deux ou plusieurs correspondants, depuis un service de messagerie.

Ainsi, toute correspondance entre deux personnes doit être protégée au titre du secret, par les opérateurs dont l'activité consiste à acheminer, transmettre ou transférer le contenu de ces correspondances. Tout comme un facteur n'a pas le droit d'ouvrir un courrier postal, le fournisseur de messagerie électronique ou le fournisseur d'accès à internet sont tenus de respecter le secret des courriers électroniques.

Ce principe de confidentialité était d'ailleurs déjà garanti par l'article L32-3 du Code des postes et des communications électroniques qui prévoyait, dans sa version antérieure à la publication de la loi pour une République numérique que « *les opérateurs, ainsi que les membres de leur personnel, sont tenus de respecter le secret des correspondances* ».

La directive européenne 2002/58 modifiée relative à la vie privée dans les communications électroniques (l'article 5.1) interdit « *à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs* ».

Le contenu des communications, c'est-à-dire des correspondances entre deux individus, est par principe confidentiel et l'obligation de garantir le secret repose sur les opérateurs de télécommunication.

Il est en revanche possible de lever le secret des correspondances, en demandant aux personnes concernées leur consentement.

Qu'est-ce qui change avec la loi pour une République numérique et son décret d'application relatif à la confidentialité des correspondances ?

L'article 68 de loi pour une République numérique précise ce que couvre le secret des correspondances. Ce secret s'applique ainsi à l'identité des correspondants, au contenu, à l'intitulé et aux pièces jointes des correspondances.

Quels sont les professionnels concernés ?

Sont désormais soumis au respect du secret des correspondances, à la fois les « *opérateurs* », c'est-à-dire les opérateurs de télécommunications essentiellement, et les « *fournisseurs de services de communication au public en ligne* », en d'autres termes, tout acteur permettant à deux personnes de correspondre en ligne. Seront notamment concernés les fournisseurs de services de messagerie électronique, de réseaux sociaux, de communication synchrone (VoIP), etc.

A quelles conditions peuvent-ils exploiter la correspondance privée ?

La loi Lemaire leur permet toutefois d'exploiter la correspondance privée, **sous réserve d'obtenir le consentement des utilisateurs et pour les seules finalités suivantes** :

- l'amélioration du service de communication au public en ligne,
- la réalisation de statistiques,
- l'utilisation des données à des fins publicitaires.

Quels sont les effets en pratique pour les opérateurs de communication électronique ou fournisseurs de service ?

La CNIL rappelle que, pour être valable, ce consentement doit être libre, spécifique et informé. Il doit en outre résulter d'un acte positif et être préalable à la collecte des données, c'est-à-dire à la réalisation du traitement.

Un consentement informé

Les opérateurs souhaitant utiliser la correspondance de leurs utilisateurs à des fins statistiques, publicitaires ou encore pour améliorer leur service devront recueillir leur consentement spécifique après les avoir informés de ce qu'ils souhaitent faire (en rappelant les mentions requises par l'article 32 de la loi Informatique et libertés).

Un consentement spécifique

La CNIL rappelle que le consentement doit être spécifique et qu'à ce titre, un consentement global pour plusieurs finalités différentes, de même que l'acceptation globale des Conditions générales d'utilisation (ou CGU) du service, **ne peuvent être considérés comme un consentement valable**.

Un consentement libre

Le consentement ne doit pas être contraint, c'est-à-dire que le refus de consentir ne doit pas empêcher la personne d'accéder au service de messagerie. Le consentement doit prendre la forme d'un acte positif des utilisateurs et ne peut donc être déduit du silence ou de l'inaction des utilisateurs. Le consentement devant être recueilli avec une périodicité d'un an, la CNIL recommande que les responsables de traitement alerte les personnes dans un délai raisonnable avant l'échéance de ce délai, pour que le renouvellement ne soit pas automatique.

Un consentement renouvelé tous les ans

La loi pour une République numérique prévoit que le consentement doit être renouvelé périodiquement, c'est-à-dire recueilli tous les ans par les opérateurs exploitant les correspondances.

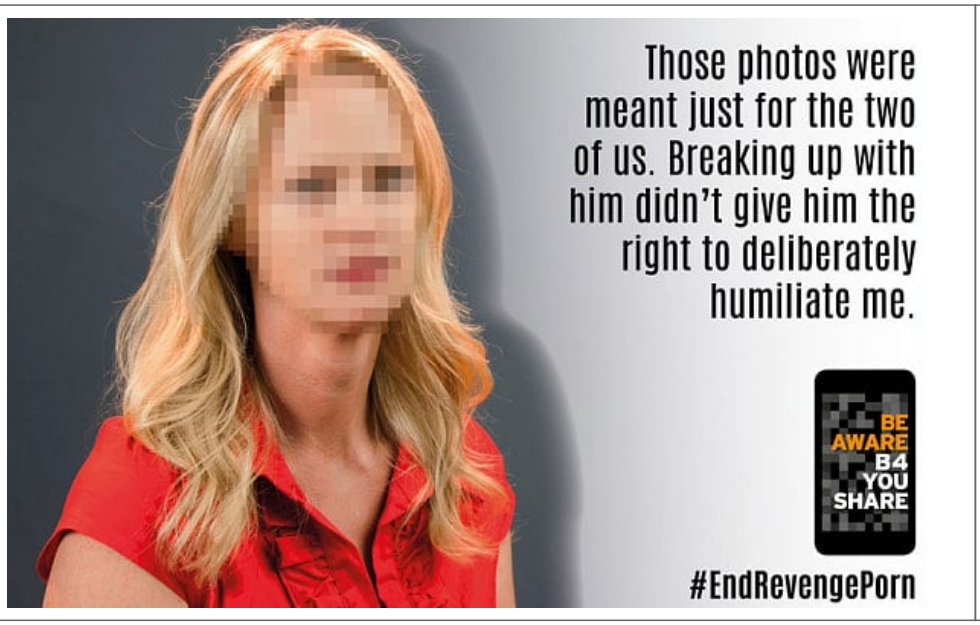
Par ailleurs, la CNIL rappelle que les traitements réalisés sur les correspondances doivent se limiter aux données collectées de manière loyale et licite. En conséquence, les traitements ne doivent produire des effets qu'à l'égard des personnes qui ont valablement consenti à la collecte de leurs données à caractère personnel issues du contenu de leurs correspondances. À titre d'exemple, les traitements opérés à des fins publicitaires et basés sur le contenu des correspondances ne doivent pas permettre à l'opérateur de cibler d'éventuelles personnes tierces dont les données personnelles apparaitraient dans la correspondance.

Enfin, la CNIL rappelle qu'une fois le règlement européen relatif à la protection des données, adopté, les responsables de traitement devront être en mesure de prouver que les personnes ont effectivement consenti au traitement et seront tenus de les informer de la possibilité de retirer leur consentement.

Réagissez à cet article

Source : *Secret des correspondances : un consentement renforcé des utilisateurs de services de communication électronique | CNIL*

Le « revenge porn » dans la loi pour une République numérique



Le « revenge porn » dans la loi pour une République numérique

---

Nous nous penchons ici sur une des nouvelles conquêtes de la loi du 7 octobre 2016 pour une République numérique.Nous avons déjà examiné certaines facettes de cette loi sur les questions d'e-réputation, notamment celle du droit à l'effacement pour les mineurs (notre actualité du 26 janvier 2017) et celle de la mort numérique (celle du 3 février). Voici à présent la prévention pénale du revenge porn, qui du reste vient de connaître une illustration judiciaire intéressante.

Par Didier FROCHOTN

Notion de *revenge porn*

On nomme sous cette élégante expression franglaise l'action qui consiste à se venger d'une personne en rendant publique des contenus pornographiques, réalisés avec ou sans accord de l'intéressé(e) mais qui n'a jamais donné son accord pour leur publication, dans le but évident de l'humilier. Il s'agit fréquemment de « retombées collatérales » d'une séparation de couple qui se passe mal. Il n'est pas nécessaire d'être footballeur professionnel pour se trouver au cœur d'une tourmente médiatique très traumatisante pour la victime, comme en témoigne certain(e)s de nos client(e)s qui en 'ont vécu une.

Le *revenge porn* face au droit

La Cour de cassation s'était déjà prononcée sur cette question le 16 mars 2016 (actualité du 18 mars) dans une affaire où elle avait alors écarté le délit pénal de publication d'image. Dans ce cas précis, la personne avait été consentante à la réalisation d'une vidéo d'ébats sexuels avec son conjoint, mais pas de sa mise en ligne après séparation.

Nous nous sommes montré quelque peu critique sur cette décision qui certes se bornait à appliquer l'interprétation stricte de la loi pénale. Nous montrions alors quelles autres voies la Cour aurait pu suivre. Et nous avions annoncé le futur renforcement de l'arsenal pénal en cas de vengeance par publication de contenus à caractère sexuel par la loi pour une République numérique alors en gestation.

Un renforcement de l'arsenal juridique pénal

L'article 67 de la loi du 7 mars 2016 est donc venu renforcer le code pénal en créant, sous les articles 226-1 et 226-2 (délit d'atteinte volontaire à l'intimité de la vie privée par transmission de propos tenus en privé ou par captation et diffusion d'image, puni d'un an de prison et de 45 000 € d'amende), un nouvel article 226-2-1 qui renforce les sanctions pénales dans les cas spécifiques de contenus à caractère sexuel…[lire la suite]

Réagissez à cet article

Source : *Le « revenge porn » dans la loi pour une République*

numérique

Comment se préparer au règlement européen sur la Protection des Données Personnelles en 6 étapes ?

	Comment se préparer au règlement européen sur la Protection des Données Personnelles en 6 étapes ?

Le 25 mai 2018, le règlement européen sera applicable. De nombreuses formalités auprès de la CNIL vont disparaître. En contrepartie, la responsabilité des organismes sera renforcée. Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

ETAPE 1 DÉSIGNER UN PILOTE

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

> En savoir plus

ETAPE 2 CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

> En savoir plus

ETAPE 3 PRIORISER LES ACTIONS À MENER

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

> En savoir plus

ETAPE 4 GÉRER LES RISQUES

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).

> En savoir plus

ETAPE 5 ORGANISER LES PROCESSUS INTERNES

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

> En savoir plus

ETAPE 6 DOCUMENTER LA CONFORMITÉ

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

> En savoir plus

…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Règlement européen : se préparer en 6 étapes | CNIL*

Avec Apple, les données des collégiens migrent aux Etats-Unis

	Avec Apple, les données des collégiens migrent aux Etats-Unis

La gestion de certains iPads des collégiens des Hauts de Seine est confiée à Apple School Manager, qui stocke les données aux États-Unis. Et cela inquiète.

En septembre 2016, le Conseil Départemental des Hauts de Seine annonçait la signature d'une convention passée avec l'Etat pour « les Collèges numériques et l'innovation pédagogique », s'inscrivant dans le Plan National Numérique de l'Etat. Cet accord prévoit, pour l'année scolaire 2016/2017, la distribution de 4500 tablettes dans différents collèges du département. Coût de l'opération : 3,1 millions d'euros dont 991 000 € cofinancés par l'Etat, soit 2,1 millions d'euros à la charge du département.
Après un appel d'offres, c'est Apple et ses iPad qui ont été choisis par l'assemblée départementale. Dans certains cas, ce déploiement se fera sur la base d'une mutualisation, c'est-à-dire qu'une tablette pourra servir à plusieurs élèves ou enseignants. Pour gérer cette mutualisation, Apple propose un outil de gestion nommé School Manager. Sur le site de la firme, on apprend que la solution permet de « *créer automatiquement des identifiants Apple gérés pour tous les élèves et le personnel, configurer les réglages d'inscription des appareils et acheter et distribuer facilement apps, livres et supports pédagogiques* ».

Des données stockées aux Etats-Unis

Oui mais voilà, ce service inquiète. En effet, « *le service Apple School Manager comporte des données à caractère personnel, relatives aux élèves et aux enseignants, qui sont hébergées sur le territoire des Etats-Unis* », peut-on lire dans une lettre du recteur de l'Académie de Versailles. Toujours sur le site d'Apple, un document relatif à « *la confidentialité des données des établissements scolaires* » souligne, dans un paragraphe sur le transfert des données à l'international : « *avec Apple School Manager, les identifiants Apple gérés, iTunes U et iCloud, les données personnelles peuvent être stockées ailleurs que dans leur pays d'origine. Où que les données soient stockées, elles sont assujetties aux mêmes normes et exigences rigoureuses en matière de stockage des données*. » Et de préciser que le transfert transatlantique des données est soumis au Safe Harbor (invalidé en octobre 2015) ou à ses successeurs, en l'occurrence le Privacy Shield (déjà contesté). Ainsi, que par « *les clauses contractuelles types de l'UE/l'Accord de Transmission à l'étranger de la Suisse, qui ont été ajoutés à l'Accord Apple School Manager* ».
Face à cette problématique de localisation des données, le rectorat explique qu'Apple School Manager doit faire l'objet « *d'une déclaration normale auprès de la CNIL et d'une information auprès des usagers* ». Au nom de l'autonomie des établissements, c'est donc aux principaux des Collèges concernés de faire cette déclaration auprès de la CNIL.

Les Hauts de Seine temporisent

Nous avons sollicité l'avis des différents protagonistes dans cette affaire. En premier lieu, le Conseil Départemental des Hauts de Seine se dit conscient du problème : « *dans le cadre du Plan numérique national des collèges, le Département des Hauts-de-Seine a remis à ce jour 3 568 tablettes personnelles à des collégiens et professeurs, sur les 4 500 prévues sur l'année scolaire 2016/2017. Le logiciel Apple School Manager n'est donc actuellement pas utilisé, puisque seules les tablettes mutualisées sont concernées par cette problématique qui retient toute l'attention du Département.* »
Il ajoute que « *les 932 tablettes restantes, qui seront mutualisées, seront remises après qu'une solution définitive soit trouvée* » (sic). Cette dernière phrase montre que la solution Apple School Manager n'est pas encore mise en œuvre et que des solutions alternatives pourraient être envisagées comme des outils de MDM (Mobile Device Management)…[lire la suite]

Réagissez à cet article

Source : *Avec Apple, les données des collégiens migrent aux Etats-Unis*