Tracfin : le renseignement financier cible la FinTech

Tracfin : le renseignement financier cible la FinTech

Financement participatif détourné, paiement mobile opaque, transactions virtuelles anonymes… Tracfin met l'accent sur les risques numériques et appelle la FinTech à coopérer. Son objectif : mieux lutter contre le blanchiment de capitaux et le financement du terrorisme.

Tracfin, la cellule française de renseignement financier, a remis ce jeudi au ministre de l'Économie et des Finances, Michel Sapin, son rapport d'analyse des risques de blanchiment de capitaux et de financement du terrorisme. Financement participatif détourné, paiement mobile opaque, transactions virtuelles anonymes… Tracfin met l'accent sur les risques numériques émergents.

Selon le rapport, *« les risques d'escroquerie dans la finance participative (crowdfunding) sont élevés, par exemple par le détournement des paiements ou par l'élaboration de fraudes du type pyramide de Ponzi »*, surtout pour les plateformes de prêt. Quant aux plateformes de dons et de cagnottes en ligne, elles sont exposées à des risques *« importants de blanchiment de capitaux et de financement du terrorisme »*,. Certes, les fonds collectés restent limités, mais ils ont tout de même été multipliés par deux entre 2014 et 2015, observe Tracfin. **196,3 millions d'euros** ont été collectés via les plateformes de prêt l'an dernier, 50,3 millions d'euros pour l'investissement et 50,2 millions d'euros pour les dons.

Cadre européen pour le financement participatif

En France, un cadre juridique dédié au financement participatif a été mis en place en 2014. Il impose aux plateformes de prêt et d'investissement le choix d'un statut de conseiller en investissement participatif (CIP), régulé par l'Autorité des marchés financiers (AMF), ou d'intermédiaire en financement participatif (IFP), régulé par l'Autorité de contrôle prudentiel et de résolution (ACPR). Ces plateformes sont donc bien assujetties au dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme (**LCB/FT**).

En revanche, la démarche restait facultative pour les plateformes de dons et les cagnottes en ligne. Mais elles seront aussi soumises à ce régime à partir de 2017, une ordonnance transposant une directive européenne dans ce domaine ayant été publiée le 2 décembre. C'est une bonne chose pour le directeur de Tracfin, Bruno Dalles, qui recommande l'adoption d'un cadre règlementaire dédié au financement participatif à l'échelle européenne. Car le cadre réglementaire national ne s'applique pas aux plateformes qui proposent, depuis l'étranger, d'effectuer des dons, prêts ou investissements…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Tracfin : le renseignement financier cible la FinTech

---

Piratage de ses comptes de réseaux sociaux. Comment réagir ?

Piratage de ses comptes de réseaux sociaux. Comment réagir ?

Vos comptes sociaux abritent une somme considérable de données personnelles. Veillez à bien les sécuriser pour éviter les piratages d'individus malveillants.

Prévenir un piratage

1.

Choisissez des mots de passe complexes, différents et non-signifiants !

Aucune personne ou ordinateur ne doit être en mesure de le deviner. La CNIL publie des conseils pour créer un mot de passe efficace, le retenir et le stocker dans une base.

2.

Ne communiquez pas votre mot de passe

Il est vivement déconseillé de communiquer votre mot de passe à une tierce personne, de l'enregistrer dans un navigateur si vous n'avez pas défini de mot de passe maître ou dans une application non sécurisée.

3.

Activez un dispositif d'alerte en cas d'intrusion

La double authentification est une option activable sur la plupart des réseaux sociaux. Lorsque vous vous connectez depuis un poste informatique inconnu, le réseau social vous demandera de confirmer l'accès en entrant un code que vous aurez reçu par sms ou par courrier électronique. D'autres fonctions proposent simplement de vous alerter si une personne extérieure tente de se connecter à votre compte depuis un terminal inconnu (PC, smartphone, tablette, mac).

4.

Déconnectez à distance les terminaux encore liés à votre compte

La encore, cette option disponible sur la plupart des réseaux sociaux vous permet d'identifier l'ensemble des terminaux avec lesquels vous vous êtes connectés à votre compte. Lorsque cela est possible, il est conseillé de désactiver le lien avec les terminaux dont vous ne vous servez plus. Une connexion identifiée depuis un navigateur inconnu ou une ville inconnue pourra vous mettre la puce à l'oreille.

5.

Désactivez les applications tierces connectées à votre compte

Il arrive que les applications tierces connectées à votre compte soient vulnérables à une attaque extérieure. Il est conseillé de désactiver les applications tierces dont vous avez autorisés l'accès par le passé et qui ne vous servent plus.

6.

Réglez vos paramètres de confidentialité

En devinant votre nom, votre fonction, votre liste d'amis, une personne mal intentionnée pourrait facilement déduire des informations qui servent à réinitialiser votre compte ou simplement à usurper votre identité afin de changer votre mot de passe par exemple.

Repérer un piratage

- votre mot de passe est invalide
- des tweets/posts imprévus sont envoyés depuis votre compte
- des messages privés sont envoyés de façon non volontaires
- des comportements inhabituels ont lieu sur votre compte sans consentement (comme suivre, se désabonner, ou bloquer)
- une notification de la part du réseau social vous informe que « Vous avez récemment changé l'adresse électronique associée à votre compte. »

Réagir en cas de piratage

1. Signalez le compte piraté auprès du réseau social
2. Demandez une réinitialisation de votre mot de passe
3. Une fois votre compte sécurisé, n'oubliez pas de parcourir les rubriques « sécurité » proposées par ces réseaux sociaux

---

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Cybercriminalité, Protection des Données Personnelles

Contactez nous

Réagissez à cet article

Original de l'article mis en page : Prévenir, repérer et réagir face au piratage de ses comptes sociaux | CNIL

Être payé pour donner le droit d'utiliser vos données personnelles ?

Être payé pour donner le droit d'utiliser vos données personnelles ?

Vos données personnelles vous appartiennent, et nul ne devrait les utiliser sans vous dédommager.

Argent contre données personnelles : un nouveau marché

Le Britannique Nicholas Oliver veut « ***faire prendre conscience aux gens que leurs données ont une valeur et qu'ils doivent en prendre soin*** ». Pour lui, pas question de laisser les géants du web comme **Facebook ou Google**, ni les médias, les agences et les annonceurs, exploiter à des fins commerciales nos données personnelles, **sans notre consentement et sans que nous puissions en tirer un éventuel bénéfice**. Sur notre dos, en somme !

« *Nous sommes […] victimes de* ***la plus formidable extorsion de valeur des temps modernes*** », estimait d'ailleurs Gaspard Koenig, du think tank libéral GénérationLibre dans le journal *Les Échos*.

Nicholas Oliver a donc décidé de créer une start-up, baptisée People.io, qui propose de **rémunérer les particuliers qui accepteraient de fournir leurs données personnelles à des entreprises…**[lire la suite]

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.

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

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les entreprises qui

utilisent vos données personnelles vont devoir payer

Le FBI a désormais le droit de pirater n’importe quel ordinateur dans le monde !

Le FBI a désormais le droit de pirater n’importe quel ordinateur dans le monde !

Le FBI est désormais doté de nouveaux pouvoirs, à savoir l'extension de ses capacités actuelles en matière de piratage informatique. Sur la base d'un mandat spécial, les agents du bureau pourront s'introduire sur n'importe quel ordinateur, situé aux États Unis mais également dans le monde.

Applicable dès aujourd'hui, la réforme est à nuancer. En effet, l'application de la **règle 41** du *Federal Rules of Criminal Procedure* (équivalent de notre code de procédure pénale) est strictement encadrée par un **juge fédéral**, qui instruit au préalable le dossier. Il s'agira d'une procédure **exceptionnelle**, la spécificité de l'affaire devant justifier de l'**opportunité** d'une telle mesure.
L'intervention reste, en effet, une **intrusion dans la vie privée des gens** *–qui ne sont pas forcément coupables de ce qui pourrait leur être reproché*. Cela n'empêche pas les politiques américains de s'inquiéter sur des atteintes aux libertés personnelles, des abus possibles ou d'éventuelles finalités politiques.
Précisons que ce pouvoir n'est pas unique en son genre, il existe déjà en France où il est actuellement renforcé du fait du plan *vigipirate* au même titre que certains pouvoirs de surveillance.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Les nouveaux pouvoirs de piratage informatique du FBI

Nouveau décret relatif au vote par voie électronique

Décret relatif au vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise.

Le décret n° 2016-1676 du 5 décembre 2016 relatif au vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise est publié au Journal Officiel du 6 décembre 2016. Il modifie le code du travail.

A retenir (DILA) : « le décret précise les modalités du vote électronique pour les élections des délégués du personnel et du comité d'entreprise prévues en l'absence d'accord. »

Consulter le décret n° 2016-1676 sur Legifrance :
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033538273&dateTexte=&categorieLien=id
[block id="24761" title="Pied de page HAUT"]

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :
• Expert en Informatique **assermenté et indépendant** ;
• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.
Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.
Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.
Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

La coopération Internationale renforcée dans le Cloud

La coopération Internationale renforcée dans le Cloud

« Le quinzième anniversaire de la Convention de Budapest sur la cybercriminalité est un tournant dans la mesure où la Convention atteint maintenant les « nuages », a déclaré le Secrétaire Général du Conseil de l'Europe Thorbjørn Jagland lors de l'inauguration de la Conférence Octopus 2016.

Les données et donc les preuves électroniques sont de plus en plus stockées sur des serveurs relevant de juridictions étrangères, inconnus ou multiples. C'est pourquoi, il peut être extrêmement difficile pour les autorités chargées de la justice pénale d'obtenir régulièrement de telles preuves. Faute de celles-ci, les délinquants qui opèrent dans le cyberespace ne peuvent être poursuivis.
Le Secrétaire Général a salué le jeu de recommandations adoptées par le Comité de la Convention sur la cybercriminalité lors de sa réunion des 14-15 novembre, dans lesquelles il voit une réponse véritable au problème de l'informatique en nuage (cloud computing). Les recommandations prévoient la négociation d'un protocole additionnel à la Convention à partir du milieu de 2017.
« La coopération entre les Etats s'est considérablement améliorée. Cela est dû pour beaucoup au travail du Comité de la Convention. Les notes d'orientation adoptées par le Comité ont aidé à préserver la pertinence et l'actualité de la Convention, à renforcer notre capacité de combattre le terrorisme, le vol d'identités ou les attaques contre des infrastructures d'informations critiques », a déclaré le Secrétaire Général, qui a invité les gouvernements à mieux protéger les droits des particuliers dans le cyberespace.
« Nous avons élaboré une sorte de « triangle dynamique » – Convention, Comité et renforcement des capacités – si bien que la Convention de Budapest reste aujourd'hui le traité international le plus important sur la cybercriminalité et la preuve électronique », a-t-il conclu.
A l'occasion de la conférence, Andorre a ratifié la Convention en présence d'Eva Descarrega Garcia, Secrétaire d'Etat andorrane à la Justice et à l'Intérieur.
68 Etats sont soit déjà parties à la Convention de Budapest, soit se sont formellement engagés à la respecter. Au moins 70 pays de plus ont pris la Convention comme source d'inspiration pour élaborer leur législation interne.
[Discours de Thorbjørn Jagland (*anglais*)]

Original de l’article mis en page : Cybercriminalité : vers un nouvel outil juridique sur la preuve électronique – News

---

Les lanceurs d’alertes dans la Loi pour une République numérique

Les lanceurs d’alertes dans la Loi pour une République numérique

---

Les lanceurs d'alertes ou « white hats » interpellent de plus en plus les medias depuis quelques années. Ces hackers éthiques interviennent dans l'informatique et le numérique, ils veillent à avertir les responsables de la sécurité des SI des vulnérabilités de leurs systèmes d'information ou de leurs sites web.

De plus, avec le développement de plates-formes de bug bounty comme YesWeHack, il était important de légaliser une pratique exposée à des sanctions pénales (ex : art. 323-1 du code pénal, 2 ans de prison et 60.000 euros d'amende). La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique vient préciser le cadre légal de leurs actions.

L'AFFAIRE DE L'ANSES ET LE VOL DE DONNÉES

Un journaliste-blogueur surnommé « Bluetouff » avait extrait, puis publié de nombreux fichiers confidentiels en pénétrant sur le site extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES). Il a été condamné par la Cour d'appel de Paris le 5 février 2014, puis par la Cour de cassation le 20 mai 2015 pour maintien frauduleux dans le SI et vol de données. Le législateur, « alerté » de cette situation, a commencé par modifier l'article 323-3 du code pénal en y ajoutant les actions d'extraire, de détenir, de reproduire, de transmettre frauduleusement des données (Loi n°2015-912 du 24 juillet 2015).

LA PREMIÈRE MOUTURE VISÉE À L'ARTICLE 20 SEPTIE DE LA LOI

C'est un amendement du 15 janvier 2016, dit « Bluetouff » qui a relancé les débats sur le sujet ayant abouti à la proposition d'ajouter un nouvel alinéa à l'article 323-1 du code pénal, ainsi rédigé :
« Toute personne qui a tenté de commettre ou commis le délit prévu au présent article est exempte de peine si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système. »

Il était censé protéger les lanceurs d'alerte lorsqu'ils veillent *« à avertir les responsables de traitement des failles dans leurs systèmes.* » Or, cette rédaction laissait dubitatifs les juristes et posait plus de questions qu'elle n'en résolvait, notamment : quelle autorité saisir et par quel canal (appel téléphonique à la police, courrier postal ou électronique à une cour d'appel ou à la CNIL, etc.) ? Que se passe-t-il après l'avertissement et surtout, si entre temps le responsable du SI a porté plainte, ou encore si le lanceur d'alertes diffuse les informations sur l'internet pour se faire de la publicité ? De plus, exemption de peine ne signifie pas non inscription au casier judiciaire de la condamnation. Pourtant, une décision du 9 septembre 2009 a jugé que tout accès non autorisé à un SI constitue un trouble manifestement illicite alors même que cela peut permettre d'éviter des atteintes ultérieures aux données ou au fonctionnement du système.

LA PROTECTION NOUVELLE DES LANCEURS D'ALERTE

L'article 47 de la nouvelle loi prévoit que le code de la défense soit complété par un article L. 2321-4 ainsi rédigé : « *Art. L. 2321-4.- Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'*article 40 du code de procédure pénale *n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données. »*
« L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée. »
« L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

L'information vise les vulnérabilités de sécurité des SI (art. 323-1) mais sans doute pas les autres délits informatiques prévus aux articles 323-2 (entraver et fausser le fonctionnement d'un SI), 323-3 (introduction de données, extraction, transmission, reproduction, suppression, modification des données) et 323-3-1 (programmes malveillants), ainsi que les infractions commises en groupe ou en bande organisée. Ces dernières infractions peuvent, en effet, causer des dommages importants au responsable du SI. L'un des points essentiels sera de déterminer les conditions de la *bonne foi* de la personne ayant détecté la vulnérabilité, étant observé que si la personne agit dans le cadre d'un programme de Bug bounty, on peut supposer que la bonne foi est présumée dans la mesure où le programme est déterminé par l'utilisateur, c'est à dire l'entreprise (idem pour la société qui réalise un Pentest).Il en va de même, si l'informateur a pénétré dans le site et qu'il s'en retire dès le moment où il s'aperçoit qu'il accède à une partie du site ou des données protégées…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs. Vous apprendre à vous protéger des pirates informatiques, vous accompagner dans votre mise en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles (RGPD). (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Les lanceurs d’alertes dans la Loi pour une République numérique

---

La loi pour une République numérique protège encore plus nos données personnelles

	La loi pour une République numérique protège encore plus nos données personnelles

---

Quels sont les apports de la loi république numérique en matière de protection des données personnelles ?

La loi pour une République numérique du 7 octobre 2016 crée de nouveaux droits informatique et libertés et permet ainsi aux individus de mieux maîtriser leurs données personnelles. Elle renforce les pouvoirs de sanctions de la CNIL et lui confie de nouvelles missions. Elle contribue également à une meilleure ouverture des données publiques.
Certaines dispositions anticipent le règlement européen sur la protection des données personnelles applicable en mai 2018.
Publiée au Journal Officiel du 8 octobre 2016, la loi pour une république numérique introduit de nombreuses dispositions directement applicables, d'autres doivent attendre la publication de décrets d'application. Nous recensons ci-dessous les dispositions d'application directe. Ce recensement sera mis à jour au fur et à mesure de la publication des décrets d'application.

De nouveaux droits pour les personnes

L'affirmation du principe de la maîtrise par l'individu de ses données
Le droit à l'autodétermination informationnelle s'inspire d'un droit similaire dégagé par la juridiction constitutionnelle allemande. Il renforce positivement les principes énoncés à l'article 1er de la loi Informatique et Libertés en affirmant la nécessaire maîtrise de l'individu sur ses données.

Le droit à l'oubli pour les mineurs
L'article 40 de la loi Informatique et libertés prévoit désormais un « droit à l'oubli » spécifique aux mineurs et **une procédure accélérée pour l'exercice de ce droit**. Lorsque la personne concernée était mineure au moment de la collecte des données, elle peut obtenir auprès des plateformes l'effacement des données problématiques « dans les meilleurs délais ».
En l'absence de réponse ou de réponse négative de la plateforme dans un délai de un mois, la personne peut saisir la CNIL qui dispose alors d'un délai de 3 semaines pour y répondre.

La possibilité d'organiser le sort de ses données personnelles après la mort
Le nouvel article 40-1 de la loi Informatique et libertés permet aux personnes de donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès.
Une personne peut être désignée pour exécuter ces directives. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés.
Ces directives sont :
• générales, lorsqu'elles portent sur l'ensemble des données concernant une personne ;
• ou particulières, lorsque ces directives ne concernent que certains traitements de données spécifiques.

Lorsque ces directives sont générales et portent sur l'ensemble des données du défunt, elles peuvent être confiées à un tiers de confiance certifié par la CNIL.

Lorsqu'il s'agit de directives particulières, elles peuvent également être confiées aux responsables de traitement (réseaux sociaux, messagerie en ligne) en cas de décès. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation.
En l'absence de directives données de son vivant par la personne, les héritiers auront la possibilité d'exercer certains droits, en particulier :
1. le droit d'accès, s'il est nécessaire pour le règlement de la succession du défunt ;
2. le droit d'opposition pour procéder à la clôture des comptes utilisateurs du défunt et s'opposer au traitement de leurs données.

La possibilité d'exercer ses droits par voie électronique
Le nouvel article 43 bis de la loi Informatique et Libertés impose, « lorsque cela est possible », de permettre à toute personne l'exercice des droits d'accès, de rectification ou d'opposition par voie électronique, si le responsable du traitement des données les a collectées par ce vecteur.

Plus d'information et de transparence sur le traitement des données.

L'information des personnes sur la durée de conservation de leurs données
L'obligation d'information prévue par l'article 32 de la loi Informatique et Libertés est renforcée. Les responsables de traitements de données doivent désormais informer les personnes de la durée de conservation des données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.

Les compétences de la CNIL confortées et élargies

Un pouvoir de sanction renforcé
Le plafond maximal des sanctions de la CNIL **passe de 150.000€ à 3 millions €** (anticipation sur l'augmentation du plafond du montant des sanctions par le règlement européen qui sera applicable le 25 mai 2018 et prévoit un plafond pouvant aller jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, 4% du chiffre d'affaires mondial).
La formation restreinte de la CNIL peut désormais ordonner que les organismes sanctionnés informent individuellement de cette sanction et à leur frais, chacune des personnes concernées.
Elle pourra également prononcer des sanctions financières sans mise en demeure préalable des organismes lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité.

Une consultation plus systématique de la CNIL.
La CNIL sera saisie pour avis sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données. Cette rédaction permettra à la CNIL d'apporter son expertise aux pouvoirs publics de manière plus systématique, alors que les textes actuels ne prévoient sa saisine que sur les dispositions relatives à la « protection » des données personnelles.

La publicité automatique des avis de la CNIL sur les projets de loi.
Cette disposition renforce la transparence sur les avis de la CNIL.

De nouvelles missions :
• **L'affirmation de sa mission de promotion de l'utilisation des technologies protectrices de la vie privée**, notamment les technologies de chiffrement des données.
• **La certification de la conformité des processus d'anonymisation** des données personnelles dans la perspective de leur mise en ligne et de leur réutilisation. L'anonymisation des bases de données est une condition essentielle à leur ouverture ou à leur partage : elle permet de prémunir les personnes des risques de ré-identification, et les acteurs (administrations émettrices de données, ré-utilisateurs, entreprises privées qui réalisent des recherches notamment statistiques), de la mise en cause de leur responsabilité en la matière. La certification ou l'homologation de méthodologies d'anonymisation ainsi que la publication de référentiels ou de méthodologies générales par la CNIL sera ainsi un gage de protection des personnes et de sécurité juridique pour les acteurs.
• **La conduite par la CNIL d'une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques.** Même si la loi Informatique et Libertés a toujours comporté une dimension éthique fondamentale, comme en témoignent tant ses conditions de création et son article 1er, que la composition de la Commission, la révolution numérique implique une réflexion élargie sur sa dimension éthique.

L'ouverture des données publiques étendue

La loi pour une république numérique ne remet pas en cause l'équilibre entre transparence administrative et protection de la vie privée et des données personnelles. En effet, les critères de communicabilité n'ont pas changé, et la publication – donc la réutilisation – est subordonnée au caractère librement communicable du document.
Pour autant, en passant d'une logique de la demande d'un accès à une logique de l'offre de données publiques, la loi vise clairement à ouvrir très largement les données publiques. La CNIL va accompagner cette ouverture, notamment en répondant aux demandes de conseil des collectivités publiques ou des réutilisateurs, puisque toute réutilisation de données personnelles est soumise au « droit commun » Informatique et Libertés. La possibilité pour la CNIL d'homologuer des méthodologies d'anonymisation constituera un élément important de cette régulation.
En matière de gouvernance de la donnée, la loi prévoit un rapprochement entre la CNIL et la CADA, à travers, notamment, une participation croisée dans les deux collèges.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Ce que change la loi pour une République numérique pour la protection des données personnelles | CNIL

Les SMS, mails, enregistrements et messages vocaux peuvent-ils être utilisés comme preuve aux prud’hommes ?

Les SMS et les mails constituent un moyen de communication courant dans le cadre des relations de travail. Les salariés échangent de cette manière avec leur supérieur hiérarchique, et vice versa.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la règlementation relative au numérique et notamment la protection des données

Personnelles. Il est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur notre page formations.

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Les SMS, mails, enregistrements et messages

vocaux peuvent-ils être utilisés comme preuve aux prud’hommes ?

Les SMS, mails, enregistrements et messages vocaux peuvent-ils être utilisés comme preuve aux prud’hommes ?

Les SMS et les mails constituent un moyen de communication courant dans le cadre des relations de travail. Les salariés échangent de cette manière avec leur supérieur hiérarchique, et vice versa.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la règlementation relative au numérique et notamment la protection des données Personnelles. Il est régulièrement invité à des **tables rondes en France et à l’étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d’informations sur notre page formations.

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article