

Les États peuvent-ils imposer aux FAI une obligation générale de conservation des données ?



Les États
peuvent-ils
imposer aux
FAI une
obligation
générale de
conservation
des données
?

Dans un arrêt, la Cour de justice de l'Union européenne considère que les États ne peuvent pas imposer une « conservation généralisée et indifférenciée » des données de connexion. Celle-ci doit se faire de façon « ciblée, limitée et avec des garde-fous.

L'accès aux données de connexion ne peut pas être « open bar ». Tel est, en somme, le sens de l'arrêt que la Cour de justice de l'Union européenne vient de rendre ce mercredi 21 décembre. Pour les magistrats, il n'est pas possible d'imposer aux fournisseurs d'accès à Internet une « *conservation généralisée et indifférenciée* » des données de connexion de leurs clients. Celle-ci doit être extrêmement ciblée et fortement délimitée pour éviter des dérives. Rappel des faits. C'était le 8 avril 2014. Dans son mémorable arrêt *Digital Rights Ireland*, la Cour de justice de l'Union européenne manifestait sa volonté jurisprudentielle de protéger les droits des internautes, en invalidant la directive européenne de 2006. Celle-ci obligeait les États membres à exiger des opérateurs qu'ils conservent un journal des données de connexion de leurs clients pour que la police et la justice puissent y avoir accès.

S'appuyant sur la Charte des droits fondamentaux de l'Union européenne, la cour jugeait que cette obligation était disproportionnée et offrait un cadre insuffisant pour la protection de la vie privée et des données personnelles des citoyens européens. Grâce à cet arrêt, plusieurs États ont suspendu ou révisé leur législation pour intégrer l'avis de la cour suprême communautaire. D'autres nations ont en revanche choisi de ne pas bouger, à l'image de la France.



CC Harald Deischinger

Sollicité dans le cadre de deux affaires jointes (C-203/15 Tele2 Sverige et C-698/15 Secretary of State for Home Department/Tom Watson e.a), l'avocat général de la Cour de justice de l'Union européenne, le Danois Henrik Saugmandsgaard Øe a considéré au mois de juillet que les États membres avaient bien le droit d'exiger la conservation de toutes les métadonnées mais uniquement s'ils se conforment aux impératifs fixés par l'arrêt *Digital Rights Ireland*.

Une analyse que la Cour de justice de l'Union européenne a refusé de suivre. Dans un arrêt rendu le 21 décembre, l'institution communautaire n'a en effet pas suivi l'avocat général. Elle déclare que les États ne peuvent pas imposer aux fournisseurs d'accès à Internet une obligation générale de conservation de données, que ces données soient relatives au trafic ou qu'elles concernent la localisation. Pour le dire autrement, l'accès aux données n'est plus « open bar »...[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 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.



Réagissez à cet article

Original de l'article mis en page : Les États ne peuvent pas imposer aux FAI une obligation générale de conservation des données – Politique – Numerama

Une cyberattaque crée une nouvelle coupure électrique en Ukraine ?



Suite à une nouvelle panne de courant, la compagnie nationale d'électricité de l'Ukraine enquête pour savoir si une attaque de cyberpirates est à l'origine du problème.

Des experts en sécurité cherchent à savoir si la panne de courant qui a affecté ce week-end certains quartiers de la capitale ukrainienne, Kiev, et la région environnante provient d'une cyberattaque. Si ce dernier point venait à être confirmé, il s'agirait du deuxième black-out causé par des pirates informatiques en Ukraine, après celle qui s'est produite en décembre 2015.

✘ L'incident a affecté les systèmes de commande d'automatisation d'un relais de puissance près de Novi Petrivtsi, un village situé au nord de Kiev, entre samedi minuit et dimanche. Cela a entraîné une perte de puissance complète pour la partie nord de Kiev sur la rive droite du Dniepr et la région environnante...

75 minutes pour rétablir le courant

Les ingénieurs d'Ukrenergo, la compagnie d'électricité ukrainienne, ont commuté l'équipement de commande en mode manuel et commencé à rétablir la puissance par palier de 30 minutes, a dit Vsevolod Kovalchuk, directeur d'Ukrenergo, dans un billet posté sur Facebook. Il a fallu 75 minutes pour restaurer toute la puissance électrique dans les zones touchées de la région, où les températures descendent jusqu'à -9 en ce moment. Une des causes suspectées est « une interférence externe à travers le réseau de données » a déclaré sans plus de précision Vsevolod Kovalchuk. Les experts en cybersécurité de la société étudient la question et publieront très bientôt un rapport.

Parmi les causes possibles de l'accident figurent le piratage et un équipement défectueux, a déclaré Ukrenergo dans un communiqué. Les autorités ukrainiennes ont été alertées et mènent une enquête approfondie. En attendant, les premières conclusions, tous les systèmes de commande ont été basculés du mode automatique au manuel, a indiqué la compagnie.

Un Etat derrière les attaques sophistiquées

Si un piratage venait à être confirmé, ce serait la seconde cyberattaque en un an contre le réseau électrique ukrainien. En décembre dernier, juste avant Noël, des pirates informatiques avaient lancé une attaque coordonnée contre trois compagnies d'électricité régionales ukrainiennes. Ils avaient réussi à couper l'alimentation de plusieurs sous-stations, provoquant des pannes d'électricité qui ont duré entre trois et six heures et touché les résidents de plusieurs régions.

A l'époque, les services de sécurité ukrainiens, le SBU, avaient attribué l'attaque à la Russie. Bien qu'il n'y ait aucune preuve définitive liant ces attaques au gouvernement russe, les cyberattaquants avaient utilisé un morceau de malware d'origine russe appelé BlackEnergy, et la complexité de l'attaque suggère l'implication d'un État. La semaine dernière, des chercheurs du fournisseur de sécurité ESET ont alerté la communauté au sujet d'attaques récentes contre le secteur financier ukrainien menées par un groupe qui partage de nombreuses similitudes avec le groupe BlackEnergy...[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 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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Une cyberattaque suspectée de causer un black-out en Ukraine – Le Monde Informatique

Que nous réserve la CyberSécurité en 2017 ?



La fin de l'année c'est aussi et surtout la période des bilans. Dans cet article, nous mettrons en évidence les cinq tendances les plus importantes tendances à venir. Qu'elles se maintiennent ou évoluent durant l'année 2017, une chose est sûre, elles risquent de donner du fil à retordre aux professionnels de la cybersécurité.

1 : intensification de la guerre de l'information

S'il y a bien une chose que la cybersécurité nous a apprise en 2016, c'est que désormais, les fuites de données peuvent être motivées aussi bien par la recherche d'un gain financier ou l'obtention d'un avantage concurrentiel que pour simplement causer des dommages dus à la divulgation d'informations privées. À titre d'exemples, le piratage du système de messagerie électronique du Comité National Démocrate (DNC) américain qui a conduit à la démission de Debbie Wassermann Schultz de son poste de présidente ; ou encore, la sécurité des serveurs de messagerie qui a miné la campagne présidentielle américaine de la candidate Hillary Clinton dans sa dernière ligne droite. Il est également inexcusable d'oublier que Sigmundur Davíð Gunnlaugsson, le Premier ministre islandais, a été contraint de démissionner en raison du scandale des Panama Papers. Les événements de ce type, qui rendent publiques de grandes quantités de données dans le cadre d'une campagne de dénonciation ou pour porter publiquement atteinte à un opposant quelconque d'un gouvernement ou d'une entreprise, seront de plus en plus fréquents. Ils continueront de perturber grandement le fonctionnement de nos institutions et ceux qui détiennent actuellement le pouvoir.

2 : l'ingérence de l'État-nation

Nous avons assisté cette année à une augmentation des accusations de violations de données orchestrées par des États-nations. À l'été 2015, l'administration Obama a décidé d'user de représailles contre la Chine pour le vol d'informations personnelles relatives à plus de 20 millions d'Américains lors du piratage des bases de données de l'Office of Personnel Management. Cette année, le sénateur américain Marco Rubio (républicain, État de Floride) a mis en garde la Russie contre les conséquences inévitables d'une ingérence de sa part dans les élections présidentielles. Il s'agit là d'une autre tendance qui se maintiendra. Les entreprises doivent donc comprendre que si elles exercent ou sont liées de par leur activité à des secteurs dont les infrastructures sont critiques (santé, finance, énergie, industrie, etc.), elles risquent d'être prises dans les tirs croisés de ces conflits.

3 : la fraude est morte, longue vie à la fraude au crédit !

Avec l'adoption des cartes à puces – notamment EMV (Europay Mastercard Visa) – qui a tendance à se généraliser, et les portefeuilles numériques tels que l'Apple Pay ou le Google Wallet qui sont de plus en plus utilisés, les fraudes directes dans les points de vente ont chuté, et cette tendance devrait se poursuivre. En revanche, si la fraude liée à des paiements à distance sans carte ne représentait que de 9 milliards d'euros en 2014, elle devrait dépasser les 18 milliards d'ici 2018. Selon l'article New Trends in Credit Card Fraud publié en 2015, les usurpateurs d'identité ont délaissé le clonage de fausses cartes de crédit associées à des comptes existants, pour se consacrer à la création de nouveaux comptes frauduleux par l'usurpation d'identité. Cette tendance devrait se poursuivre, et la fraude en ligne augmenter. Le cybercrime ne disparaît jamais, il se déplace simplement vers les voies qui lui opposent le moins de résistance. Cela signifie, et que les fraudeurs s'attaqueront directement aux systèmes de paiement des sites Web.

4 : l'Internet des objets (IdO)

Cela fait maintenant deux ans que les experts prédisent l'émergence d'un ensemble de risques inhérents à l'Internet des objets. Les prédictions sur la cybersécurité de l'IdO ont déjà commencé à se réaliser en 2016. Cela est en grande partie dû à l'adoption massive des appareils connectés d'une part par les consommateurs, mais aussi par les entreprises. En effet, d'après l'enquête internationale portant sur les décideurs et l'IdO conduite par IDC, environ 31 % des entreprises ont lancé une initiative relative à l'IdO, et 43 % d'entre elles prévoient le déploiement d'appareils connectés dans les douze prochains mois. La plupart des entreprises ne considèrent pas ces initiatives comme des essais, mais bien comme faisant partie d'un déploiement stratégique à part entière. Cette situation va considérablement empirer. L'un des principaux défis de l'IdO n'est pas lié à la sécurisation de ces appareils par les entreprises, mais plutôt au fait que les fabricants livrent des appareils intrinsèquement vulnérables : soit ils sont trop souvent livrés avec des mots de passe par défaut qui n'ont pas besoin d'être modifiés par les utilisateurs, soit la communication avec les appareils ne requiert pas une authentification de niveau suffisant ; ou encore, les mises à jour des firmwares s'exécutent sans vérification adéquate des signatures. Et la liste des défauts de ces appareils n'en finit pas de s'allonger. Les entreprises continueront d'être touchées par des attaques directement imputables aux vulnérabilités de l'IdO, que ce soit par des attaques par déni de service distribué (attaques DDoS), ou par le biais d'intrusions sur leurs réseaux, rendues possibles par les « faiblesses » inhérentes de l'IdO.

5 : bouleversements de la réglementation...[\[lire la suite\]](#)

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 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 83841 84) Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



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

- Audits Sécurité (ISO 27001) ;
- Expertises techniques et judiciaires (avis techniques, recherche de preuves téléphoniques, disques durs, e-mails, contenus, détournements de données...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Auteurs de la loi sur la Sécurité des Systèmes) ;
- 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 : Les grandes tendances 2017 de la cybersécurité, Le Cercle

Les mails de Clinton piratés par des «hackeurs russes», stratégie de diversion ?



Les mails de Clinton
piratés par des
«hackeurs russes»
stratégie
de diversion ?

Les Etats-Unis utilisent la Russie comme un «ennemi commode», dont l'existence est indispensable pour entretenir leur complexe militaro-industriel, explique Jean-Robert Raviot, professeur des études russes.

RT France : Barack Obama a donné vendredi passé sa dernière conférence de presse en tant que président, où il a évoqué la Russie et les hackers russes qui auraient piraté les comptes du Parti démocrate américain alors que, selon la déclaration du procureur général des Etats-Unis, il n'y a pas de preuve de l'origine de ces attaques. Pourquoi alors accuser la Russie ?

Jean-Robert Raviot (J.-R. R.) : Il faut chercher la réponse dans une logique qui n'est pas proprement en Russie, mais plutôt Washington. C'est à dire qu'on assiste aujourd'hui à un tir de barrage contre Donald Trump de la part du Parti démocrate et d'un certain nombre de gens qui soutenaient la candidature de Hillary Clinton. Dans cette affaire il y a trois points qui soulèvent question pour moi. Premièrement, sur un plan technique – pourquoi est-ce que ce hacking, s'il est avéré qu'il a été repéré par la CIA, n'est-il pas rendu public ? Et surtout, pourquoi la NSA, qui en principe devrait avoir une vision assez claire des opérations de hacking sur le territoire américain, ne s'est-elle pas prononcée ?

de croire qu'il faut remarquer que personne de la NSA n'a donné son avis sur la question. Pour moi, ça met déjà un gros doute sur la réalité de ce hacking, sur la preuve qu'on peut avoir que des hackers russes ont agi pour prendre possession de ces mails de Podesta et ceux de Clinton. C'est un point technique, mais qui me semble important quand-même. Parce que cette question n'est pas résolue, et personne ne la pose vraiment.

On a cherché à discréditer Bernie Sanders. C'est ça le problème

deuxième point, comme je l'analyse, c'est la volonté de brouiller un peu l'information. Le fond de l'affaire c'est ce qu'il y a dans ces mails, et la preuve, que du côté de Hillary Clinton, on a cherché à discréditer Bernie Sanders. C'est ça le problème. On voit très clairement dans ces mails une opération interne du Parti démocrate visant tout simplement à mettre de côté Bernie Sanders, à lui mettre des bâtons dans les roues dans cette campagne électorale et dans cette primaire. C'est très clairement avéré. Le fait d'accuser la Russie ou le Kremlin ou les hackers russes d'avoir monté cette opération, permet de détourner l'attention du fond des mails.



Barack Obama exige un rapport sur le piratage, dont les résultats ne seraient pas rendus publics

Du coup, plus personne ne parle de la réalité de ce qui est dit dans ces mails, et du fait qu'ils ne sont pas rédigés par les hackers, mais par les gens qui ont tenu ces correspondances. Je dirais, c'est un moyen de détourner l'attention du grand public sur un problème qui n'est pas le même. C'est comme le vieux proverbe chinois : «Le sage montre la lune, et l'idiot regarde le doigt qui montre la lune». C'est absolument une stratégie de diversion.

La volonté c'est de se servir d'un ennemi assez commode, parce que c'est l'ennemi historique de la guerre froide – ça permet de mobiliser des récits qui sont déjà écrits et qui résonnent dans les têtes des gens

La troisième point c'est la véritable volonté de la part d'un groupe dirigeant actuellement aux Etats-Unis, qui est autour d'Obama, autour du Parti démocrate, de Hillary Clinton et leurs soutiens, d'essayer de ramasser un maximum d'arguments. Pour l'instant, je pense qu'il y a des gens qui préparent l'impeachment de Trump. Je pense que c'est un peu rapide de dire ça – pour le moment, il n'est pas encore investi, on ne peut pas faire la destitution de quelqu'un qui n'est pas encore investi. Mais je pense que l'objectif c'est de faire une campagne, de tenter d'orienter le vote des grands électeurs et de faire en sorte qu'ils ne votent pas pour Trump.

RT France : Pourquoi ont-ils choisi Vladimir Poutine et la Russie, et non pas la Chine, par exemple, en guise de bouc émissaire ?

« M. R. : Parce que la Russie, je dirais, a été désignée comme l'ennemi principal non seulement des États-Unis, mais aussi de l'Alliance atlantique. Rappelez-vous, quand en juillet 2016, au sommet de Varsovie de l'OTAN, on a désigné la Russie comme l'ennemi principal, alors que le djihadisme apparaît à peine dans le texte. C'est quand-même incroyable. La volonté c'est de se servir d'un ennemi qui existe, un ennemi qui est assez commode, parce que c'est l'ennemi historique de la guerre froide – ça permet de mobiliser des récits qui sont déjà écrits et qui résonnent dans les têtes des gens. C'est un ennemi familier, en quelque sorte. En même temps, l'image de Poutine permet d'associer cette image à un homme fort, anti-Obama, pas une personnalité, on peut facilement l'opposer aux dirigeants occidentaux. Et puis, ça résonne aussi bien dans le contexte de la guerre en Syrie et surtout de la guerre qu'on veut mener. C'est la narration de cette guerre qu'on veut imposer, c'est-à-dire, un soutien certainement des forces anti-Assad et anti-régime, de continuer ces opérations de « régime change », qui ont commencé en 2003, tout en s'appuyant sur le pays qui s'y oppose pour l'instant militairement, d'une manière directe. [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 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

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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisée 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 cybersécurité ;
(Autorisation de la DCTEP n°03 BO (0001) 04)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Original de l'article mis en page : Les «hackeurs russes», une stratégie de diversion pour oublier le contenu des mails de Clinton – RT en français

5 à 10% du budget d'une entreprise devrait être consacrée à la cybersécurité



5 à 10% du budget d'une entreprise devrait être consacrée à la cybersécurité

La sécurité a un cout mais ce n'est pas grand-chose comparé au prix à payer lorsqu'on est victime d'une attaque informatique.

Toutes les entreprises sont des cibles potentielles mais les secteurs des nouvelles technologies, des systèmes d'information, des médias, du transport et de logistique, de la grande distribution sont exposés à des pertes financières lourdes.

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 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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Les 5 chiffres à connaître de la cybersécurité – BeRecruited

La Poste livrera ses colis par drones dans le Var



Dans le Var, après deux ans d'essais, La Poste a obtenu de Direction Générale de l'Aviation Civile (DGAC) le droit d'ouvrir une ligne commerciale régulière de 15 km pour la distribution de colis par drones. Elle se situera entre Saint-Maximin-La-Sainte-Baume et Pourrières....[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 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 sur cette page.



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.



[Contactez-nous](#)

Réagissez à cet article

La Poste livrera ses colis par drones dans le Var



Dans le Var, après deux ans d'essais, La Poste a obtenu de Direction Générale de l'Aviation Civile (DGAC) le droit d'ouvrir une ligne commerciale régulière de 15 km pour la distribution de colis par drones. Elle se situera entre Saint-Maximin-La-Sainte-Baume et Pourrières....[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 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 sur cette page.



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.



[Contactez-nous](#)

Réagissez à cet article

Vote électronique aux élections professionnelles

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
LE NET EXPERT AUDITS & EXPERTISES	EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES LE NET EXPERT fr	LE NET EXPERT MISES EN CONFORMITÉ	SPY DETECTION Services de détection de logiciels espions	LE NET EXPERT FORMATIONS	LE NET EXPERT ARNAQUES & PIRATAGES
Denis JACOPINI vous informe		Vote électronique aux élections professionnelles			

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.

Désormais, le chef d'une entreprise employant au moins 11 salariés peut recourir au vote électronique pour ses élections professionnelles et ce même en l'absence d'un accord collectif.

Il peut dorénavant décider de fixer lui-même les modalités du vote électronique, sous réserve de respecter les conditions fixées par le décret du 5 décembre 2016.

L'employeur d'au moins 11 salarié peut ainsi décider de recourir au vote électronique pour les élections partielles se déroulant en cours de mandat.

Il choisit, dans ce cas, si le vote électronique interdit ou pas le vote à bulletin secret sous enveloppe.

Le chef d'une entreprise employant au moins 11 salariés doit établir un cahier des charges respectant les dispositions réglementaires relatives au vote électronique et le tenir à la disposition des salariés sur le lieu de travail et sur l'intranet de l'entreprise.

Attention : pendant le déroulement du scrutin, aucun résultat partiel n'est accessible.

Seul, le nombre de votants peut, si l'employeur le prévoit, être révélé au cours du scrutin.

Par **Carole Vercheyre-Grard**

Avocat au Barreau de Paris

Source juritravail.com

[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

Le Règlement Général sur la Protection des Données (RGPD) en détail



Après quatre années d'âpres négociations, les États Membres de l'Union Européenne sont enfin convenus d'un texte venant moderniser la directive 1995/46/CE du 24 octobre 1995, laquelle datait des débuts d'Internet. Mais, contrairement à une directive, le Règlement adopté le 8 avril 2016 par le Conseil de l'Europe puis, le 16 avril, par le Parlement européen, est d'application directe et s'imposera aux États Membres à compter du 25 mai 2018, sans qu'il soit besoin de le transposer dans les législations nationales.

Le processus d'élaboration du texte, long et émaillé de près de 4000 amendements, a mis au monde un texte très long – plus de 200 pages – comportant 99 articles introduits par 173 considérants. Intitulé « Règlement n°2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », le texte résultant, complexe et technique, est particulièrement difficile à aborder par les entreprises et les administrations, lesquelles sont pourtant les principaux acteurs visés par le texte. Ainsi, dans un article du 18 octobre 2016, le journal La Tribune écrivait que « 96% des entreprises des trois principales économies européennes (France, Allemagne, Royaume-Uni) ne comprennent pas encore clairement le Règlement général de protection des données (RGPD) (...) Selon une étude publiée ce mardi par la société de sécurité informatique Symantec, 92% des dirigeants et décideurs français s'inquiètent de ne pas être en conformité au moment de l'entrée en vigueur de la RGPD » !

Les acteurs du traitement de données vont donc devoir investir considérablement pour se mettre à niveau de la nouvelle réglementation, d'autant que toutes les entreprises du monde traitant des données personnelles de citoyens européens sont concernées par le Règlement. Nous nous proposons, à travers cet article, d'exposer les principales nouveautés du texte sous une forme compréhensible pour le non-initié. Nous dresserons au préalable un tableau général des intentions du texte (I) avant d'insister sur ses innovations principales (II).

I- Présentation générale du RGPD

Le but déclaré du texte est de renforcer le contrôle des citoyens européens sur l'utilisation de leurs données personnelles, tout en simplifiant, en l'unifiant, la réglementation pour les entreprises. Les citoyens pourront désormais réclamer contre l'utilisation abusive de leurs données auprès d'une autorité unique, chargée de la protection des données, plutôt que de devoir le faire auprès de l'entreprise détentrice de leurs données. Les particuliers pourront également se joindre à des recours collectifs via des organisations représentatives qui, si la loi nationale les y autorise, pourront agir de leur propre initiative. Le RGPD développe ainsi considérablement les droits reconnus à la personne dont les données sont collectées. Ainsi, des trois droits reconnus à la personne par la loi Informatique et Liberté (opposition au traitement sous réserve de motif légitime, droit d'accès/communication aux données, droit de rectification/suppression), l'on passe à 11 droits (droit à une information complète en langage clair, droit à l'oubli, droit à la limitation du traitement, droit à la portabilité des données, droit d'opposition (notamment au profilage), etc.). D'une manière générale, la personne concernée dispose d'un droit étendu et facilité à accéder aux données à caractère personnel qui la concernent et le texte réaffirme les principes essentiels de la protection de la vie privée :

- Restriction d'utilisation ;
- Minimisation des données ;
- Précision ;
- Limitation du stockage ;
- Intégrité ;
- Confidentialité.

Les entreprises sont incitées à privilégier l'utilisation de pseudonymes avant et pendant le traitement des données pour en garantir la protection (concept de la prise en compte du respect de la vie privée dès la conception). La « pseudonymisation » consiste à s'assurer que les données sont conservées sous une forme ne permettant pas l'identification directe d'un individu sans l'aide d'informations supplémentaires.

II- Principales mesures du RGPD

1. Réalisation d'une analyse d'impact avant la mise en place d'un traitement de données
Avant la mise en place d'un traitement de données pouvant présenter des risques pour la protection des données personnelles, l'entreprise devra réaliser une analyse d'impact : « *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.* » (Article 35 du Règlement)
Le RGPD introduit ainsi le concept de prise en compte du respect de la vie privée dès la conception du traitement : les différentes obligations pesant sur la collecte des données doivent être prises en compte dès la conception du traitement de données (« *privacy by design and by default* »).

2. Consentement clair et explicite à la collecte des données
La directive 1995/46/CE donnait une définition du consentement à la collecte des données, laquelle a été transposée de manière très hétérogène dans les législations nationales, certaines exigeant un consentement explicite, d'autres décidant qu'un consentement implicite était suffisant. Notre loi Informatique et Liberté se contente ainsi de définir des cas dans lesquels le consentement devrait être explicite. Le Règlement vient unifier une fois pour toute cette définition au onzième point de son article 4 consacré aux définitions, en définissant le consentement comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». Ce consentement doit donc être expressif. Il doit résulter d'un acte positif. La personne doit réellement avoir été mise devant la nécessité de donner son accord au traitement. Ainsi, dans son considérant n°32, le Règlement précise qu'« *il ne saurait dès lors y avoir de consentement en cas de silence, de case cochée par défaut ou d'inactivité.* » Plus encore, la charge de la preuve du consentement pèse sur le responsable du traitement (article 7, 1°). En outre, la personne dont les données sont collectées peut retirer son consentement à tout moment (article 7, 3°). Malgré cela, le Règlement prévoit un certain nombre de cas pour lesquels le traitement demeure licite même sans consentement (article 6, b) à f)) :

- Lorsque ce traitement est nécessaire à l'exécution d'un contrat accepté par la personne ;
- Lorsque le traitement découle d'une obligation légale ;
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne ;
- Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
- Tout autre intérêt légitime du responsable du traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne, en particulier s'il s'agit d'un enfant.

3. Accès facilité de la personne à ses données
Les personnes dont les données sont collectées disposent de droits à la rectification, à l'effacement des données et à l'oubli : « *la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données la concernant et le responsable du traitement a l'obligation d'effacer ces données dans les meilleurs délais* » (Article 17), et ce pour six motifs : les données ne sont plus nécessaires, la personne concernée retire son consentement, la personne concernée s'oppose au traitement à des fins de prospection, les données ont fait l'objet d'un traitement illicite, les données doivent être effacées pour respecter une obligation légale, ou encore les données ont été collectées dans le cadre d'une offre de service à destinations de mineurs.

4. Notification des violations de données personnelles (« Data Breach Notification »)
A l'heure actuelle, les différentes directives européennes font peser sur les entreprises du secteur de la télécommunication l'obligation d'informer les autorités en cas « *d'accès non autorisé* » à des données personnelles. En clair, lors d'un piratage, le Règlement, quant à lui, généralise cette obligation de signalement à l'ensemble des responsables de traitement, et ce au plus tard 72 heures après la découverte du problème (Article 33). Bien entendu, il faut que le problème atteigne une certaine gravité pour qu'il soit nécessaire de le rapporter, et tout va donc dépendre de la détermination du seuil à partir duquel le signalement devient obligatoire. L'article 34 du Règlement indique que ce signalement devra intervenir « *lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.* » L'emploi du mot « *élevé* » laisse donc place à appréciation et donnera donc probablement lieu au développement d'une jurisprudence abondante. Les personnes concernées par la violation des données doivent également être notifiées dans les meilleurs délais, sauf si des mesures de protection ont été mises en œuvre ou seront prises ultérieurement.

5. La création et la maintenance d'un registre des traitements devient obligatoire
Aux termes de l'article 30 du RGPD, un registre détaillé des traitements doit désormais être obligatoirement conservé non seulement par le responsable du traitement mais également par ses éventuels sous-traitants. Ce registre doit pouvoir être mis à tout moment à disposition des autorités de contrôle. Le texte insiste ainsi sur la responsabilité du contrôleur des données, lequel est responsable de la conformité du traitement avec le Règlement et doit être, à tout moment, en mesure de la démontrer. Lorsque le traitement de données est délégué par le responsable du traitement à un sous-traitant, ou « *data processor* », même situé hors de l'Union Européenne, celui-ci a désormais les mêmes obligations que le responsable du traitement, y compris la désignation d'un délégué à la protection des données, et ce même dans le cas d'un traitement de données gratuit.

6. Création des délégués à la protection des données (Data Protection Officer)
Si notre loi Informatique et Liberté, et ses mises à jour, ont créé le Correspondant Informatique et Liberté (le « *CIL* »), le Règlement, quant à lui, rend obligatoire dans certains cas la nomination d'un délégué à la protection des données (DPO ou, en anglais, DPO : Data Protection Officer) pour les organismes privés ou publics dont « *les activités de base (...) exigent un suivi régulier et systématique à grande échelle des personnes concernées* » ou lorsque « *le traitement est effectué par une autorité publique ou un organisme public* » (article 37), à l'exception des juridictions. Ce délégué n'est obligatoire que dans certains cas, mais il est fortement recommandé de le nommer systématiquement puisque toute entreprise ou administration doit être capable à tout moment de rendre compte à l'autorité de contrôle de l'état de ses traitements de données. Le rôle du délégué à la protection des données sera de garantir la conformité des traitements de données avec les principes de protection de la sphère privée, tels que fixés par le RGPD, ainsi que de gérer les relations entre les personnes concernées (employés, clients) et les autorités de surveillance.

7. Le transfert des données est soumis à vérification et peut être demandé par la personne elle-même
Les transferts de données personnelles vers des pays étrangers sont désormais soumis à la vérification des garanties offertes par les lois de ce pays pour préserver un niveau de sécurité équivalent pour les données. L'article 45 du Règlement prévoit que, dans l'idéal, le pays destinataire devra être listé par la Commission européenne. A défaut, des clauses de garantie spéciales devront être prévues dans les contrats, outre la possibilité de recourir à des codes de conduite, des certifications et autres labels. Auquel cas, il ne sera pas nécessaire d'obtenir une autorisation auprès de l'autorité nationale du pays d'origine des données. En outre, l'article 49 du Règlement prévoit que, si le traitement nécessitait de recueillir le consentement de la personne, alors celle-ci devra être informée du transfert de ses données et des risques que présentent l'opération. Ceci, bien entendu, afin de permettre à la personne de revenir éventuellement sur son consentement. Enfin, les personnes dont les données sont collectées disposent elles-mêmes d'un droit à demander le transfert des données les concernant (ou « *droit à la portabilité des données* ») vers un autre fournisseur de services : « *Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle* » (Article 20).

8. Restriction du profilage automatisé servant de base à une décision
L'article 21 du Règlement dispose que « *La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* », sauf si ce traitement est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, ou bien que la décision est autorisée par le droit de l'Union européenne, ou bien encore que le consentement explicite de la personne concernée a été recueilli en amont.

9. Recours et aggravation considérable des sanctions
La directive 1995/46/CE prévoyait jusqu'ici simplement la possibilité, pour la personne dont les droits ont été violés, de recourir aux tribunaux et d'obtenir du responsable du traitement réparation de son préjudice. Le Règlement prévoit quant à lui un « *droit à un recours effectif* » (articles 78 et 79) et un « *droit à réparation* » (article 82). Il définit des règles de compétences des juridictions se substituant aux règles de droit international privé des États Membres et détermine les amendes qui devront être délivrées par les autorités nationales de contrôle (article 83). Or, les amendes mises en place par le Règlement sont considérables, puisqu'elles peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial ! Le risque qui pèse sur les entreprises imprudentes est donc très sérieux...[lire la suite]

Notre métier :
Nous proposons des services d'accompagnement sur plusieurs niveaux :
1/ Au niveau des utilisateurs qui, face à la résistance au changement, doivent comprendre l'intérêt des démarches de mise en conformité des traitements des données personnelles, pour favoriser leur implication et faciliter la mission du Correspondant aux Données Personnelles.
1'/ Au niveau des utilisateurs encore peu sensibilisés les utilisateurs aux différentes formes d'attaques et d'arnaques informatiques (cybercriminalité) dont les établissements sont très largement victimes. Les services chargés de gérer les fournisseurs sont fortement incités à suivre notamment un module sur les arnaques aux FQV et à voir leurs procédures auditées et probablement améliorées.
2/ Au niveau de l'établissement complet afin de faire un état des lieux des traitements concernés et un audit des mesures de sécurité en place et à faire évoluer pour les rendre acceptables vis à vis de la Réglementation relative aux Données Personnelles.
3/ Au niveau du futur CIL ou du futur DPO afin de lui faire découvrir ses missions, l'accompagner dans sa prise de fonction et l'accompagner au fil des changements.

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>



Réagissez à cet article

Original de l'article mis en page : RGPD : le Règlement Général sur la Protection des Données qui bouleverse la loi Informatique et Liberté. Par Bernard Rineau, Avocat, et Julien Marcel, Juriste.

Vigilance – faux appels passés au nom de la CNIL

	Vigilance – faux appels passés au nom de la CNIL
---	---

Vigilance – faux appels passés au nom de la CNIL



Des entreprises ont reçu, ces derniers jours, des appels téléphoniques de personnes se faisant passer pour la CNIL et prétextant devoir envoyer des documents.

Ces appels frauduleux ont pour but de collecter des informations sur votre organisation, et notamment l'adresse mail de dirigeants (directeur informatique, directeur des achats, etc.), pour préparer une attaque informatique (rançongiciel / ransomware) ou une escroquerie financière (« arnaque au Président »).

N'y répondez pas ! En cas de doute, vous pouvez contacter la CNIL au 01 53 73 22 22

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 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.



[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Vigilance – faux appels passés au nom de la CNIL | CNIL