

# Les entreprises européennes bientôt obligées de signaler toute cyber-attaque ? | Le Net Expert Informatique



Les entreprises européennes bientôt obligées de signaler toute cyber-attaque ?

**Les entreprises du domaine des nouvelles technologies opérant en Europe pourraient devoir systématiquement reporter toute intrusion sur leurs installations informatiques. Une directive devrait étendre cette obligation au secteur du numérique.** Depuis 2013, l'Europe mène des discussions autour d'un texte visant à obliger les entreprises des secteurs de l'énergie, des transports, de la santé ou des services financiers à implémenter des mesures de sécurité minimales pour leurs installations informatiques. Baptisée NIS (pour Network and Information Security), cette directive implique surtout à ces mêmes professionnels de rapporter aux autorités compétentes tout incident informatique (cyber-attaque, intrusion, perte de données...).

Selon Reuters, cette directive pourrait être étendue à de nouveaux secteurs, à savoir à l'ensemble du domaine des nouvelles technologies. A terme, **ces sociétés qu'elles soient majeures ou non pourraient être soumises à ce devoir de divulgation en cas d'attaque informatique.**

A ce jour, certaines obligations incombent déjà aux opérateurs de réseaux d'importance vitale (eau, électricité...) mais également aux opérateurs de télécommunications. Ces derniers doivent par exemple signaler à la Cnil d'éventuelles pertes ou fuites concernant les informations personnelles de leurs clients.

Ce type d'obligation pourrait donc être étendu à davantage de sociétés. Ce volet doit toutefois être discuté devant les institutions communautaires ainsi que les Etats membres. Ces derniers devraient faire part de leurs critiques au sujet d'une extension trop large de ce texte à l'ensemble du secteur du numérique.

#### **Un débat encore vif et des critiques toujours présentes**

La question de la communication en cas de faille de sécurité reste majeure. Les exemples de fuites de données massives, comme celui de Sony, ont montré l'importance de tenir informer les personnes concernées mais aussi les autorités, pour qu'elles puissent éventuellement agir.

En Europe, et notamment en France, la question reste également pertinente. Comme nous le rapportions suite à une conférence sur le sujet, certaines entreprises préfèrent rester discrètes quant à leurs dispositifs et les relations entre « hackers blancs » peuvent rapidement tourner à l'incompréhension.

C'est pourquoi de nombreux professionnels, ou leurs représentants, critiquent une extension trop large des obligations de notification des failles de sécurité. Ces derniers craignent que ce type de contrainte nuise à la compétitivité des entreprises, ou n'entraîne un jeu du chat et de la souris peu profitable aux professionnels.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

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

Contactez-nous

---

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://pro.clubic.com/it-business/securite-et-donnees/actualite-776250-directive-nis.html>  
Par Olivier Robillart

# Bientôt un « carnet de correspondance numérique » pour les collégiens et lycéens | Le Net Expert Informatique

**Bientôt un « carnet de correspondance numérique » pour les collégiens et lycéens**

Le gouvernement a publié la semaine dernière un arrêté autorisant la création d'un téléservice censé permettre aux parents « d'être informés, à distance, des événements de vie scolaire liés aux absences, aux retards, aux punitions et aux sanctions » infligées à leur(s) enfant(s). Un véritable carnet de correspondance dématérialisé se dessine ainsi, alors que le plan pour le numérique à l'école est attendu pour la rentrée 2016.

Durant toute l'année scolaire, de nombreuses informations pourront être consignées dans ce fichier concernant les élèves de la sixième à la terminale : absences, retards, retenues, exclusions de cours, blâmes, avertissements, etc. ainsi que leurs motifs et dates. Ces informations seront accessibles via Internet au jeune concerné ainsi qu'à ses parents, de même qu'aux personnels du collège et lycée en question (enseignants, assistants d'éducation, conseiller principal d'éducation, chef d'établissement). Le tout sera toutefois effacé une fois le temps des grandes vacances venu, à la fin de chaque année scolaire.

L'objectif ? Améliorer l'information des familles et la communication avec l'établissement d'enseignement, notamment afin de mieux prévenir le décrochage scolaire. Pour autant, ce dispositif ne sera pas déployé systématiquement dans tous les collèges et lycées. Si l'arrêté permet dès à présent une mise en œuvre au niveau national, ce téléservice sera uniquement proposé par les établissements volontaires. De surcroit, chaque parent aura le droit de ne pas activer le compte de son enfant.

#### **Une phase d'évaluation dans cinq académies, avant une généralisation progressive**

Contacté, le ministère de l'Éducation nationale n'était pas en mesure de répondre dans l'immédiat à nos questions concernant le calendrier de mise en place de ce téléservice. L'exécutif a cependant indiqué à la CNIL qu'un test devrait tout d'abord être mené « dans cinq académies ». Il semble ainsi fort probable que la Rue de Grenelle suive une feuille de route similaire à celle prévue pour le récent dispositif de télépaiement des frais de cantine et d'internat, dont la généralisation devrait avoir lieu à partir de la rentrée 2016, également après une phase d'expérimentations (voir ancien article NextImpact).

Saisie pour avis, la CNIL a d'autre part prévenu le ministère de l'Éducation nationale que « les établissements devront continuer de mettre à disposition des responsables légaux qui ne seraient pas en capacité d'accéder au téléservice proposé, ou qui ne souhaiteraient pas l'utiliser, un autre moyen d'accès aux données traitées dans le téléservice ». Les explications concernant ce recours seront adossées au courrier envoyé aux parents afin de leur présenter ce dispositif « et leur attribuer un identifiant et un mot de passe provisoires », qu'ils devront changer lors de leur première connexion.

La gardienne des données personnelles a enfin invité les pouvoirs publics à être très vigilants en matière de sécurité, au-delà de l'utilisation de protocoles HTTPS et de mots de passe complexes (huit caractères minimum, avec chiffres et lettres). La CNIL souligne en effet que « l'impact sur la vie privée des élèves en cas de dysfonctionnement d'un téléservice portant sur les absences, les retards, les punitions et les sanctions pouvant être élevé, il est nécessaire que tous les établissements scolaires garantissent un niveau de sécurité satisfaisant afin d'assurer à tous les élèves du second degré une même protection ». Le ministère de l'Éducation nationale a ainsi été prié d'alerter les principaux et proviseurs sur ce point en particulier.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

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

Contactez-nous

---

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.nextinpc.com/news/96066-bientot-carnet-correspondance-numerique-pour-collegiens-et-lyceens.htm>

# **Vie privée et données**

# personnelles sous Windows 10 : les astuces de la Cnil pour vous protéger | Le Net Expert Informatique



Vie privée et données personnelles sous Windows 10 : les astuces de la Cnil pour vous protéger

La Commission nationale de l'informatique et des libertés (Cnil) a diffusé lundi 10 août un communiqué pour aider les utilisateurs du flambant neuf Windows 10 à protéger leurs données personnelles.

Au cœur d'une polémique depuis l'adoption d'une nouvelle politique sur la collecte des données privées, le dernier système d'exploitation de Microsoft s'est vu attaqué ces derniers jours par des utilisateurs mais aussi par Marine Le Pen qui dénonçait « l'espionnage généralisé des ordinateurs des Français ».

La présidente du FN avait d'ailleurs interpellé la Cnil « pour analyser les conséquences de Windows 10 sur la vie privée des Français » et demandé des mesures « afin que Microsoft se conforme à la loi française sur la protection de la vie privée. »

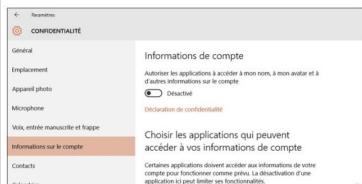
Rien de tel pour l'heure mais l'organisme propose à défaut la série de réglages ci-dessous pour « limiter la communication de vos informations à l'éditeur et à ses partenaires. »

- Cliquez sur le logo Windows en bas à gauche puis sur « Paramètres ». Sélectionnez alors le menu « confidentialité » où vous pourrez modifier les principales fonctionnalités qui collectent des données :



- Pour limiter le plus l'envoi de vos données, vous pouvez systématiquement tout désactiver.

- Par défaut la géo-localisation de votre poste est activée. Il est recommandé de la désactiver depuis l'onglet « Emplacement » .



- Vous pouvez désactiver complètement la collecte de données ou empêcher certaines applications d'y accéder. Notamment pour l'Appareil photo, le Microphone, les Informations de Compte, les Contacts, la Calendrier, la Messagerie, les communications Radio et la synchronisation avec les Autres appareils.

- Cortana, l'assistante embarquée dans Windows 10, a besoin d'accéder à plusieurs types d'informations pour fonctionner. Vous pouvez désactiver Cortana soit en cliquant sur l'icône de Cortana (le cercle) soit directement depuis la barre des tâches, soit depuis le menu démarrer. En cliquant sur le livre puis sur « Paramètres » de Cortana.



- Si vous disposez d'un compte connecté qui synchronise vos paramètres entre les différents terminaux équipés de Windows 10, vous pouvez désactiver cette synchronisation (et la collecte des données associées), en allant dans la fenêtre de « Paramètres » et en cliquant sur « Comptes » .



Nous organisons régulièrement des **actions de sensibilisation ou de formation au risque informatique**, à l'**hygiène informatique**, à la **cybercriminalité** et à la **mise en conformité** auprès de la **CNIL**. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : [http://www.huffingtonpost.fr/2015/08/10/vie-privee-donnees-personnelles-windows-10-astuces-cnil\\_n\\_7965788.html](http://www.huffingtonpost.fr/2015/08/10/vie-privee-donnees-personnelles-windows-10-astuces-cnil_n_7965788.html)

---

# Fuite d'une ébauche du projet de loi numérique d'Axelle Lemaire | Le Net Expert Informatique

**Fuite d'une ébauche du projet de loi numérique d'Axelle Lemaire**

Si la version « bêta » du projet de loi numérique n'a toujours pas été publiée (et ce alors qu'Axelle Lemaire avait indiqué que ce serait le cas « avant la fin du mois de juin »), Contexte vient de publier une version de travail du texte élaboré sous la houlette de Bercy. Ce document non définitif nous permet d'en savoir davantage sur la façon dont le gouvernement pourrait concrétiser ses ambitions.

L'ébauche diffusée par nos confrères date de début juillet, avant que la piste d'une seconde loi relative au numérique – et portée cette fois par le ministre de l'Économie, Emmanuel Macron – ne soit confirmée par le gouvernement. « Selon nos informations, le texte a évolué depuis, et n'est toujours pas complètement stabilisé. Les réunions interministérielles de validation n'ont pas encore commencé » insiste d'ailleurs le journaliste Samuel Le Goff, pour bien faire comprendre que beaucoup de choses risquent de bouger d'ici à la publication de l'avant-projet de loi censé être soumis aux commentaires des internautes cet été.

Cette version de travail, longue d'une trentaine de pages, contient malgré tout plus de 80 articles. On y retrouve les principales mesures distillées au fil du temps par la secrétaire d'État au Numérique, Axelle Lemaire, ou même par Manuel Valls. Tour d'horizon.

#### Open Data

Ouverture par défaut des données publiques détenues par l'administration. L'État, les collectivités territoriales et les personnes chargées d'une mission de service public seraient tenus de diffuser automatiquement leurs documents administratifs communicables au sens de la loi CADA, dès lors que ceux-ci existent au format électronique. Aucune référence au format de mise en ligne de ces documents ne figure cependant dans cette version de travail. L'entrée en vigueur de ces dispositions est par ailleurs progressive : dans les six mois pour des « bases de données de référence définies par un arrêté du Premier ministre », puis deux ans pour les documents administratifs reçus ou produits après la promulgation de la loi, et enfin cinq ans pour l'ensemble des documents.

Principe de gratuité. La réutilisation d'informations publiques deviendrait gratuite, également par défaut. Des redevances pourront toujours être réclamées par des administrations, à condition toutefois que « le coût de la reproduction ou de la numérisation des documents administratifs concernés ou l'anonymisation des informations qu'ils contiennent représente une part significative de leurs ressources ». Un registre public serait spécialement créé afin de rassembler toutes les informations relatives à ces différentes redevances.

Création d'un « service public de la donnée ». Sous la houlette de l'Administrateur général des données, dont les missions sont gravées dans le marbre, ce service public de la donnée aurait pour objectif de faciliter la circulation de données entre administrations. Pour la première fois, il est prévu que des décrets puissent exiger « la transmission de données à l'administrateur général des données, lorsque cette transmission est nécessaire à la constitution ou à la mise à jour des données de référence ».

Statut pour les « données d'intérêt général ». Les délégués de services publics ou les organisations recevant des subventions de plus d'un million d'euros pourraient être contraintes de mettre en Open Data certaines données produites dans le cadre de leur mission, financée sur deniers publics. L'ouverture de données purement privées (environnement, énergie...) pourrait également être exigée par les pouvoirs publics, dès lors qu'il y aurait un « motif d'intérêt général, tenant notamment à leur contribution déterminante à la mise en œuvre d'une politique publique, à la recherche [publique] ou au développement d'activités économiques nouvelles ». Ces dispositions risquent toutefois d'évoluer suite aux travaux menés par la mission Cytermann (voir notre article).

#### Ouverture du code source des logiciels développés par l'État

Les « codes source des logiciels » figureront expressément parmi la liste des informations publiques considérées communicables au sens de la loi CADA.

#### Protection des données personnelles

Plusieurs articles ont été rédigés afin que chaque utilisateur d'un service en ligne puisse obtenir la copie des données collectées à son égard, dans « un format électronique ouvert et permettant une réutilisation effective de ces données ». Des dispositions spécifiques aux emails ont également été insérées.

#### Renforcement des missions la CNIL

L'institution pourrait être « obligatoirement consultée sur tout projet de loi ou de décret comportant des dispositions relatives à la protection des données à caractère personnel ou au traitement de telles données ». Elle serait même autorisée à « prendre l'initiative de donner un avis » sur toute question relative à la protection des données personnelles, notamment en direction du législateur.

#### Plus de pouvoirs pour la CNIL

Les sanctions prononcées par la Commission pourraient devenir bien plus dissuasives pour les géants du numérique : jusqu'à 3 millions d'euros ou, pour les entreprises, 5 % de leur « chiffre d'affaires annuel mondial ». On serait ainsi bien loin des 300 000 euros maximums prévus actuellement (et uniquement en cas de manquements répétés...). En cas d'urgence, la CNIL pourrait d'autre part ordonner au responsable d'un traitement de respecter la loi Informatique et Libertés dans un délai de 24 heures, contre 5 jours actuellement.

#### Action collective pour les litiges relatifs aux données personnelles

Sur le modèle des nouvelles actions de groupe, des internautes pourraient saisir les juridictions civiles par le biais notamment d'associations de consommateurs, et ce « afin d'obtenir la cessation d'une violation » à la loi Informatique et Libertés. Assez curieusement, ce dispositif ne fonctionnerait pas pour les traitements de données personnelles mis en œuvre dans le cadre d'un service public administratif.

#### Droit à l'oubli pour les mineurs

Le fait qu'une personne ait moins de 18 ans au moment où une donnée la concernant est collectée serait un « motif légitime » justifiant l'arrêt de son traitement, « sauf si la personne mineure était une personnalité publique ».

#### Droit de « mort numérique »

Chaque internaute pourrait laisser des directives concernant le devenir de ses données personnelles, en cas de décès. La personne désignée (ou, à défaut, les héritiers) auraient ensuite le pouvoir de se tourner vers les réseaux sociaux ou autres services en ligne pour obtenir par exemple la suppression des données ou du compte du défunt, etc.

#### Des pistes très variées

**Neutralité du Net.** Posant le principe que l'exploitant d'un réseau de communication électronique n'a « ni la connaissance ni le contrôle des informations reçues ou transmises par des tiers », des restrictions ne pourraient être mises en œuvre « que dans le respect des principes de non-discrimination, de proportionnalité, de nécessité et de transparence lorsque le niveau de qualité du service n'est pas garanti ».

**Définition positive du domaine public.** L'ébauche diffusée par Contexte comprend un article qui reconnaît expressément un « domaine public informationnel », composé premièrement des « informations, données, faits, idées, principes et découvertes, dès lors qu'ils ont fait l'objet d'une divulgation publique » ; deuxièmement des « objets qui ne sont pas couverts par les droits prévus dans le Code de la propriété intellectuelle ou dont la durée de protection légale a expiré » ; et troisièmement des « documents administratifs diffusés publiquement par l'État, les collectivités territoriales, etc.

De nombreux autres sujets sont abordés, tels que la régulation des jeux d'argent en ligne, le renforcement des pouvoirs de l'ARCEP (le régulateur des télécoms), la loyauté des plateformes, etc. Sauf que certains de ces sujets auront plus vraisemblablement leur place dans l'éventuel projet de loi « Macron II », dont les mesures devraient être davantage tournées vers l'aspect économique. Résultat dans quelques jours, si le gouvernement se décide à publier (enfin) la version « bêta » du projet de loi numérique d'Axelle Lemaire.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoins d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 01 19 71 79 12

formateur n°93 84 03041 84

---

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

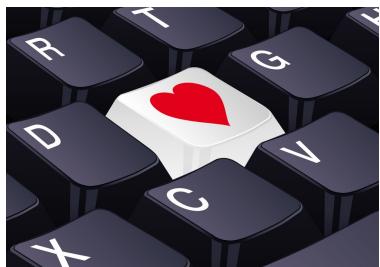
Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

---

# La Cnil met en demeure 13 sites de rencontre | Le Net Expert Informatique



**La Cnil met en demeure 13 sites de rencontre**

**Meetic, Attractive World ou Adopte un mec figurent dans une liste de 13 sites de rencontre mis en demeure par la Cnil pour leur mauvaise gestion des données de leurs membres.**

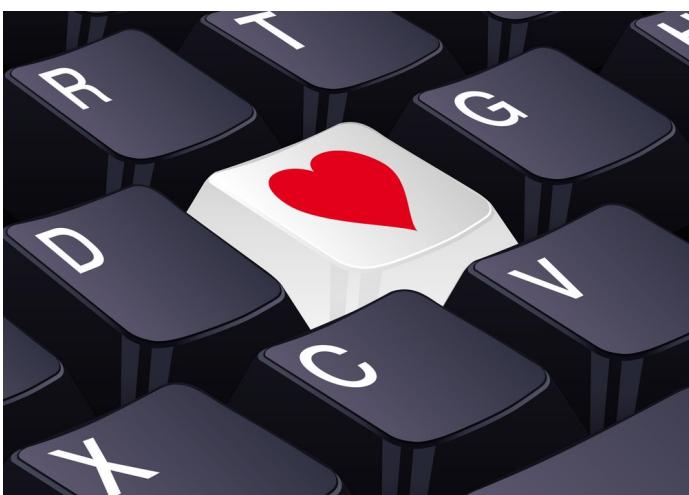
La Cnil veut éviter un scénario à la Ashley Madison en France. Ce site américain de rencontres extra-conjugales a été piraté la semaine dernière. Les données de quelque 37,5 millions de membres, aussi sensibles soient-elles, ont été dérobées. Alors la Commission nationale de l'informatique et des libertés a mené l'enquête auprès de plusieurs sites de rencontre... et annonce la mise en demeure de 13 d'entre eux.

Meetic, Attractive World, Adopte un mec, Easyflirt, Rencontre obèse, Destidyll, Forcegay, Mektoube, Jdream, Feujworld, Marmite love, Gauche rencontre, Celibest. C'est la liste retenue par la Commission, qui leur reproche à tous « de nombreux manquements à la loi informatique et libertés ».

Les voici :

- ne pas recueillir le consentement exprès des personnes pour la collecte de données sensibles, comme celles relatives à la vie et aux pratiques sexuelles, aux origines ethniques, aux convictions et pratiques religieuses ou aux opinions politiques ;
- ne pas supprimer des données de membres ayant pourtant demandé leur désinscription ou ayant cessé d'utiliser leurs comptes depuis une longue durée ;
- mettre en œuvre des fichiers afin d'exclure des personnes de l'accès au service sans avoir procédé à des demandes d'autorisation auprès de la Cnil ;
- ne pas informer correctement les internautes de leurs droits (accès, suppression, rectification) ni des conditions dans lesquelles des cookies sont déposés sur leur ordinateur.

Dépourvue de pouvoir de sanction, la Cnil peut désigner un rapporteur qui décidera, lui, d'une peine –



Crédit : Pic Rider (Fotolia)

#### **Le spectre d'une mauvaise pub**

Concrètement, ce sont les sociétés éditrices (8 au total) des sites de rencontre qui sont mises en demeure. Habituellement, une telle procédure n'est pas rendue publique par la Cnil. Une exception que justifie la Commission par la « sensibilité des données en cause » ainsi que « le nombre de personnes concernées ».

Les entreprises visées ont un délai de trois mois pour se conformer à la loi. « La clôture de chacune des procédures fera également l'objet d'une publicité », agite la Cnil, pour les motiver à améliorer leur politique de gestion des données. Dans le cas contraire, elle désignera un rapporteur chargé d'étudier des sanctions pouvant atteindre 300 000 euros selon Les Echos. Mais surtout, une mauvaise publicité leur sera faite.

---

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

Contactez-nous

---

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://pro.clubic.com/legislation-loi-internet/cnil/actualite-775064-cnil-sites-rencontre.html>  
Par Thomas Pontiroli

---

# Boulanger, épingleé par la Cnil pour des commentaires sur un fichier client | Le Net Expert Informatique



**La Cnil a mis en demeure la société Boulanger, dont les employés ont quelque peu abusé de l'espace libre laissé au sein d'un fichier client. Plusieurs commentaires insultants ont été constatés par la Commission, qui laisse 3 mois à la société pour se mettre en règle.**

Peut-on inscrire n'importe quoi dans le champ commentaire d'un fichier client ? Pas vraiment : la Cnil a ainsi annoncé aujourd'hui avoir épingle l'enseigne Boulanger suite à une plainte lui ayant signalé des commentaires injurieux dans ses fichiers clients.

Sur son site, la Cnil explique avoir effectué un contrôle sur place doublé d'un contrôle en ligne suite à un dépôt de plainte, qui lui a permis de constater des pratiques contrevenant à la loi Informatique et Libertés. « Les fichiers de la société comportaient de nombreux commentaires excessifs sur ses clients, comme par exemple « n'a pas de cerveau », « cliente avec problème cardiaque », « client alcoolique » ou encore des propos insultants » rapporte ainsi la Cnil, qui explique avoir mis en demeure Boulanger, sommé de se mettre en conformité avec la loi sous trois mois.

#### **La Cnil veut faire un exemple**

La Cnil explique avoir relevé pas moins de 5828 commentaires désobligeants parmi les fichiers clients de Boulanger. La société est également épingle pour non-respect des règles encadrant l'usage des cookies : la société manquait à son obligation de prévenir l'utilisateur de l'utilisation de cookies pour le tracking et la Cnil relève également la mise en place « de certains cookies à finalité publicitaire [ayant] une durée de vie pouvant aller jusqu'à 15 ans. » Pas de chance pour Boulanger, la Cnil explique avoir choisi de mettre en avant cette procédure « afin d'appeler notamment l'attention des entreprises sur la nécessité de ne pas enregistrer de commentaires excessifs dans leurs fichiers clients. » Il fallait faire un exemple et la Cnil précise que cette mise en demeure n'est pas une sanction, mais rappelle que si Boulanger ne se met pas en règle, une nouvelle procédure pourrait être initiée à l'encontre de Boulanger. Via son compte Twitter, la marque s'est excusé et promet de remédier à la situation.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

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

Contactez-nous

---

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.zdnet.fr/actualites/boulanger-epingle-par-la-cnil-pour-des-commentaires-sur-un-fichier-client-39822914.htm>

# **Etude d'impacts sur la vie**

# privée : découvrez la méthode | Le Net Expert Informatique

17

**Etude d'impacts sur la vie privée : suivez la méthode de la CNIL**

La CNIL publie sa méthode pour mener des PIA (Privacy Impact Assessment) pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits.

#### De l'application de bonnes pratiques de sécurité à une véritable mise en conformité

La Loi informatique et libertés (article 34), impose aux responsables de traitement de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».

Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.

Pour aider les TPE et PME dans cette étude, la CNIL a publié en 2010 un premier guide sécurité. Celui-ci présente sous forme de fiches thématiques les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement des données personnelles.

En juin 2012, la CNIL publiait un autre guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

#### Une méthode plus rapide, plus facile à appliquer et plus outillée

Ce guide a été révisé afin d'être plus en phase avec le projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.

La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL.

#### Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :

1.les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quelles que soient la nature, la gravité et la vraisemblance des risques encourus ;

2. la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.

#### Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :

- 1.étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
- 2.étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
- 3.étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
- 4.validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.

L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

PIA, LA MÉTHODE  
PIA, L'OUTILLAGE

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

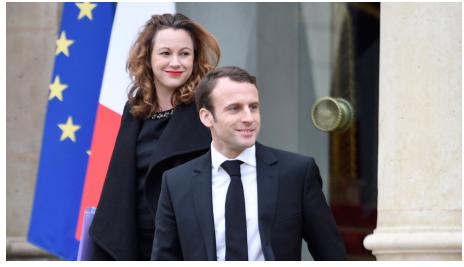
Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur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

Contactez-nous

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

Source : [http://www.newspress.fr/Communiqué\\_FR\\_289793\\_1332.aspx](http://www.newspress.fr/Communiqué_FR_289793_1332.aspx)

# Bercy devra gérer non pas une, mais deux lois numériques | Le Net Expert Informatique



Bercy devra gérer non pas une, mais deux lois humériques

**La loi numérique, tout le monde en parle. Même le chef de l'Etat a abordé le sujet lors de l'interview du 14 juillet. Désormais, il semble probable qu'au lieu d'un texte il y en ait deux. Un signé Macron pour la croissance, l'autre signé Axelle Lemaire pour les libertés.**

La question revient à chaque fois qu'un journaliste rencontre un responsable gouvernemental proche du dossier. « Où en sommes-nous de la loi numérique dont on parle depuis 2013 ? » La réponse est toujours la même, ou presque : « Nous y travaillons, nous vous tiendrons informé quand nous aurons avancé ». Rien n'est vraiment officiel mais en fait, il n'y aura pas une loi, mais deux. L'une sur la transformation numérique de l'économie, l'autre sur les libertés individuelles.

Lors de la traditionnelle interview du 14 juillet, le chef de l'Etat y a fait une allusion. « Je vais préparer une loi sur le numérique, tout ce qui est activités nouvelles, tout ce qui peut provoquer de l'emploi ». Le message s'adresse clairement à Emmanuel Macron, ministre de l'économie, de l'Industrie et du Numérique.

Dès le lendemain, lors d'un point presse, le ministre est revenu sur le sujet. Sans entrer dans les détails, il a simplement précisé que les premières propositions seront faites au plus tard début 2016. Et pour calmer les impatients, il a prévenu qu'il prendra le temps nécessaire pour l'élaborer. Et en effet l'exercice promet d'être délicat.

Emmanuel Macron est parfaitement conscient du levier que représente le numérique en matière de création d'emploi. Mais il doit composer entre une nouvelle économie qui bouscule les règles des entreprises traditionnelles. Tandis que ces dernières se trouvent, elles, confrontées à une concurrence qu'elles estiment déloyale, voire illégale selon les cas.

#### **Une loi Macron 2 pour la transformation numérique**

Dans son message, François Hollande a été plutôt clair: « il faut qu'il n'y ait rien dans nos règles, dans nos formalités qui puisse entraver ». La guerre entre Uber et les taxis est l'un des exemples les plus frappants de la crainte que génère le potentiel des nouvelles technologies. Ce sera donc à Emmanuel Macron de gérer ce dossier dans une loi qui a déjà un nom: Macron 2.

Autres sujets d'importance, les données personnelles et les libertés individuelles face aux géants du Net. Ces sujets devraient faire parti d'un second texte qui sera cette fois sous la responsabilité d'Axelle Lemaire. Le cœur de ce projet devrait donner plus de poids à la Cnil dont le pouvoir, notamment celui de sanctionner, doit être renforcé. En janvier 2015, sa présidente, Isabelle Falque-Pierrotin faisait déjà des propositions sur le contenu du texte.

Mais la présidente de la Cnil est également présidente des Cnil européennes, connues sous le nom de « Groupe de l'article 29 » et dans ce cadre, elle rappelle que le texte devra être compatible avec le projet de règlement européen. « La législation sur les données personnelles ayant une portée économique croissante, les modifications éventuelles ne doivent pas créer de distorsion entre pays de l'Union. » Le cadre est posé. Reste désormais à savoir quand Axelle Lemaire présentera cette loi. Avant ou après celle d'Emmanuel Macron?

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

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

Contactez-nous

---

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://bfmbusiness.bfmtv.com/entreprise/bercy-devra-gerer-non-pas-une-mais-deux-lois-numeriques-902051.html>  
Par Pascal Samama

---

# Prévention des risques : les dispositifs d'alerte à la population | Le Net Expert Informatique

Prévention des risques : les dispositifs d'alerte à la population

**Face aux risques (inondation, canicule, attaque terroriste, incident nucléaire, épidémie...) susceptibles de mettre en danger les populations, les maires peuvent constituer deux registres nominatifs destinés à faciliter les secours. La Commission nationale de l'informatique et des libertés (Cnil) fournit un cadre à la constitution de ces registres qui ne doivent pas être prétextes à la création de « fichiers de population ».**

L'utilisation des ces registres est strictement limitée aux secours déclenchés par le maire en cas d'alerte. Les habitants doivent avoir sollicité leur inscription par une démarche volontaire.

**Pour la collecte des informations nécessaires, la Cnil a établi deux formulaires :**

l'un au titre du « plan d'alerte et d'urgence au profit des personnes âgées et des personnes handicapées en cas de risques exceptionnels ». Il s'agit d'une reprise du « registre canicule » prévu par le décret n° 2004-926 « canicule », abrogé par le décret n° 2005-1135 ; (<http://www.courrierdesmaires.fr/wp-content/uploads/2015/06/plan-urgence-formulaire-collecte-modele.doc>) l'autre au titre du « plan communal de sauvegarde » (PCS), dispositif d'alerte générale à la population pour faire face à la réalisation de risques connus auxquels est soumis un territoire communal (décret n° 2005-1156).

(<http://www.courrierdesmaires.fr/wp-content/uploads/2015/06/pcs-formulaire-collecte-modele.doc>)

Les registres de population ainsi constitués collectent donc des données personnelles volontairement transmises par les personnes concernées. Celles qui n'y sont pas inscrites ne sont évidemment pas exclues du bénéfice des secours qui seront alors déclenchés.

A noter. Si la collecte de données de santé, souvent constatée, est par principe excessive et possible de sanctions pénales, une description objective des capacités des personnes sur ces registres semble néanmoins pertinente afin de prévoir le mode d'évacuation et le matériel de premiers secours.

Le maire, responsable de traitement, doit garantir la confidentialité et la sécurité des données. Toute personne accédant aux données du registre est tenue au secret. Les données personnelles ne peuvent en aucun cas être utilisées à d'autres fins que celle de constituer et déclencher le dispositif d'alerte.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

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

Contactez-nous

---

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.courrierdesmaires.fr/51257/prevention-des-risques-les-dispositifs-dalerte-a-la-population/>

---

# Hyperconnexion du corps humain : 3 règles pour ne pas faire n'importe quoi | Le Net Expert Informatique

**Hyperconnexion du corps humain : 3 règles pour ne pas faire n'importe quoi**

Face au déploiement des objets connectés au corps humain, qui permettent de recueillir des données de santé, utilisateurs et industriels doivent être particulièrement vigilants, nous explique Nathalie Dreyfus, conseil en propriété industrielle, Dreyfus & Associés, expert près la cour d'appel de Paris et à l'OMPI.

Bracelets, montres, balances connectés.. la santé envahit les magasins spécialisés. Au-delà de leur côté ludique, ces objets permettent aux entreprises de recueillir de très nombreuses données sur leurs utilisateurs : rythme cardiaque, nombre de pas effectués par jour, quantité et qualité du sommeil, taux de sucre dans les larmes, taux d'alcoolémie ou tension artérielle...

Ce mouvement de collecte massive de données – le big data – n'en est qu'à son début, selon la Cnil. En 2017, un utilisateur de smartphone sur deux aura installé au moins une application dédiée à son bien-être et à sa santé.

Les données recueillies sont traitées par de nombreuses entreprises qui les exploitent afin de mieux connaître leurs clients. Une pratique intrusive, qui doit susciter la vigilance des utilisateurs, mais aussi des industriels. En effet, leur responsabilité peut-être engagée. Les données recueillies, liées à la santé, ont un caractère sensible et font l'objet d'une protection renforcée. Ainsi, leur collecte et leur traitement, soumis à un contrôle accru, doivent être autorisés. Mais certaines données – celles se rapportant en général au bien-être –, échappent à une demande d'autorisation préalable grâce aux normes simplifiées. Attention cependant car la frontière entre bien-être et santé est particulièrement ténue.

Pour assurer leur sécurité juridique, les industriels du secteur mettent en place quelques règles.

#### 1. RESPECTER LE CADRE LÉGAL ET LE RAPPORT DE LA CNIL SUR LA PRATIQUE DU « QUANTIFIED SELF »

Le rapport de la Cnil, déposé fin mai 2014, intitulé 'Le corps, nouvel objet connecté', traite des problèmes liés aux données personnelles de santé issues des applications et objets de mesure de soi (quantified self). Ces pratiques consistent généralement à mesurer et à comparer avec d'autres, des variables de notre mode de vie (nutrition, exercice physique, sommeil...). La pratique du « quantified self » va continuer à s'imposer, le corps humain étant de plus en plus connecté dans ses fonctions biologiques.

Le « quantified self » constitue donc un marché d'avenir pour les professionnels. Des assureurs américains ont déjà annoncé leur souhait d'utiliser les objets connectés dans le suivi de leurs clients et la prise en compte des données dans l'indemnisation en cas de dommage. La Cnil s'inquiète des nombreux risques potentiels, tels que l'exploitation commerciale abusive des données personnelles et l'intrusion dans la vie privée des utilisateurs. Nul doute pourtant que la Commission, appuyée par le G29 et la Commissaire européenne Viviane Reding, auront à cœur de protéger ces données médicales. Dans l'attente – et face aux lois françaises et européennes très protectrices, particulièrement en ce qui concerne les données sensibles – les industriels développant des produits liés à la santé doivent veiller à rester dans les clous lors de la collecte.

#### 2. MISER SUR LE « CLIENT EMPOWERMENT » POUR GAGNER LA CONFIANCE DES CONSOMMATEURS

Ce mouvement donne davantage de pouvoirs de contrôle au client. Il permet de rééquilibrer la relation entre l'entreprise collectrice de données et l'usager qui a souvent l'impression d'être négligé par les professionnels. Cette prise de pouvoir peut aussi permettre la patrimonialisation des données à condition d'obtenir le consentement direct du client. Cela ouvre aux industriels la possibilité de commercialiser les données collectées.

#### 3. SE CONFORMER AUX PRINCIPES DE « PRIVACY BY DESIGN »

Le concept de « privacy by design » propose de faire de la protection de la vie privée de l'utilisateur une caractéristique majeure de l'objet afin « d'assurer la protection de la vie privée en l'intégrant dans les normes de conception des technologies, pratiques internes et infrastructures matérielles ». Les données recueillies ne sont alors pas extensivement partagées ou revendues. En intégrant ce concept au cahier des charges de l'objet connecté, l'industriel gagnera la confiance des clients et se démarquera aussi de ses concurrents.

#### TOUT N'EST PAS PERMIS

La pratique du « quantified self » va continuer à s'imposer, le corps humain étant de plus en plus connecté dans ses fonctions biologiques. Elle constitue donc un marché d'avenir pour les professionnels. Des assureurs américains ont ainsi déjà annoncé leur souhait d'utiliser les objets connectés dans le suivi de leurs clients et la prise en compte des données dans l'indemnisation en cas de dommage. La Cnil s'inquiète des nombreux risques potentiels, tels que l'exploitation commerciale abusive des données personnelles et l'intrusion dans la vie privée des utilisateurs. Nul doute pourtant que la Commission, appuyée par le G29 et la Commissaire européenne Viviane Reding, auront à cœur de protéger ces données médicales. Dans l'attente, face aux lois françaises et européennes très protectrices, particulièrement en ce qui concerne les données sensibles, les industriels développant des produits liés à la santé doivent tenir compte du fait que tout n'est pas permis.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

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

Contactez-nous

---

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.usine-digitale.fr/article/hyperconnexion-du-corps-humain-3-regles-pour-ne-pas-faire-n-importe-quoi.N335953>  
Par Nathalie Dreyfus, conseil en propriété industrielle, Dreyfus & Associés, expert près la cour d'appel de Paris et à l'OMPI