Les CNIL en Europe et le G29 : comment ça marche ?

	Les CNIL en Europe et le G29 : comment ça marche ?

L’utilisation de l’Internet pose de nombreux problèmes en termes d’utilisation des données personnelles des usagers du réseau. Pour tenter de gérer au mieux ces notions et éviter les débordements, plusieurs CNIL ont été créées en Europe. Un autre groupe, appelé « G29 », travaille également sur ces sujets. Qu’en est-il exactement, comment ces organismes fonctionnent-ils, quel est leur champ d’action et tout ceci fonctionne-t-il de façon efficace in fine ?…

La France a été un des tous premiers pays à établir une loi homogène et globale de protection des données personnelles et de la vie privée. La fameuse loi « informatique et libertés » a ainsi vu le jour en 1978 dans le prolongement de nombreux travaux et de quelques scandales. Comme souvent en France, une nouvelle loi s’accompagne d’une agence ou d’une commission composée de nombreux représentants, parlementaires et fonctionnaires. Quand l’Europe a accepté de légiférer à son tour sur la question de la protection des données personnelles en 1995, à la demande des pays latins et germains, la création d’équivalents de la CNIL dans chaque pays devenait une évidence. C’est ainsi que sont nées les autorités de protection des données personnelles en Europe.

Les CNIL dans chaque pays
La souveraineté d’un pays se traduit principalement par l’édiction de politiques et de lois propres à un territoire donné. Pourtant, dans le cadre juridique de l’Union européenne, les pays doivent « transposer » des directives qui sont des lignes directrices. Ainsi, dans le cadre de la directive de 1995, tous les pays de l’UE avaient l’obligation de créer des « CNIL » locales.
Dans ce cadre, les pays ont adopté des législations parfois différentes mais ressemblantes : l’Espagne a créé une autorité particulièrement présente et respectée, imposant une interprétation restrictive et très protectrice des données personnelles, pendant que certains pays de l’Est instauraient des autorités souples et peu dotées. Certains, comme le Luxembourg, demandaient l’assistance de la France pour former son personnel, de telle manière qu’aujourd’hui, la CNPD luxembourgeoise ressemble au petit frère de la CNIL. Enfin, un pays fédéral comme l’Allemagne connait un système où les länder ont un pouvoir certain au regard de la loi allemande.
Lire la suite….

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://recherche-referencement.abondance.com/2015/02/les-cnil-en-europe-et-le-g29-comment-ca.html

---

Remise des trophées du 1er concours EDUCNUM Opération Vie privée à la CNIL

Remise des trophées du 1er concours EDUCNUM Opération Vie privée à la CNIL

Le 28 janvier 2015, lors de la journée européenne de protection des données, le collectif Educnum a remis à la CNIL les prix aux lauréats du premier concours Educnum en présence de Mme Najat Vallaud-Belkacem, Ministre de l'Education nationale, de l'Enseignement supérieur et de la Recherche.

L'ambition des trophées
Pour que le web reste un espace d'échange et d'inspiration, mais aussi de respect de la vie privée, le collectif pour l'éducation au numérique a lancé le 13 octobre 2014 un concours pour les étudiants.

Son objectif :
• sensibiliser les plus jeunes, de l'école primaire au lycée, aux bons usages du web, par un dialogue intergénérationnel ;
• susciter et valoriser la créativité des étudiants ;
• mettre en lumière et donner vie à des projets innovants.

Les étudiants avaient carte blanche pour participer : application mobile, dataviz, goodies ou kit de survie sur les réseaux sociaux, tous les projets étaient les bienvenus.

Les lauréats
25 projets ont été présentés à l'issue de 3 mois de concours.
Le Grand Prix du Jury avec une dotation de 7000 euros est remis à l'équipe du Master 2 « Droit, économie et gestion de l'audiovisuel » à la Sorbonne, pour le projet Les aventures croustillantes de Prince Chip.
Le Prix Spécial du Jury avec une dotation de 3000 euros est attribué à l'équipe de l'Ecole Boulle pour le projet Data Fiction, le site dont vous êtes le héros. Vivre l'aventure, faire réfléchir, accompagner sont au cœur de ces projets qui placent le jeune public au cœur de l'action.

Les projets récompensés
« Prince Chip » Appelle à la vigilance des « âges » pour les 6/10 ans
La pédagogie sur les bonnes pratiques à adopter sur le web passe ici par un divertissement dans l'univers familier des fruits et légumes. Elle repose sur l'identification à un personnage attachant et l'utilisation d'une technique moderne, le stop motion. Le webdocumentaire Les Aventures croustillantes de Prince Chip offre aux adultes un outil d'accompagnement pour parler aux plus jeunes, dès leurs premiers pas sur le net. Unanimité du jury pour remettre le Grand Prix à une fiction qui donne la frite !
Visionner le projet
Pour Serge Tisseron, psychiatre et co-auteur de l'avis de l'Académie des Sciences « L'enfant et l'écran » et membre du jury : « C'est un bonheur de découvrir comment, sur Internet, un méchant poivron peut se faire passer pour une jolie tomate ! Je fais le pari que les autres épisodes sauront toucher avec une égale efficacité la part d'enfance qui existe chez chacun, et à tout âge. »

Devenir héros de son propres site avec « Data fiction » pour les 12/18 ans
Le serious game Data Fiction fait de l'internaute un héros. En partant des outils et services numériques utilisés par les jeunes au quotidien, le projet révèle à l'utilisateur l'exposition de ses données. Ce jeu en trois étapes (découverte, appropriation, tutoriel) fait le pari de l'expérience pour sensibiliser : incité à dépasser ses limites, le jeune devient acteur. Les compétences-métier des étudiants en design de l'Ecole Boulle ont été particulièrement saluées par le jury, « une véritable œuvre d'art ! ».
Visionner le projet

Pour Stéphane Distinguin, Président de Cap Digital et membre du jury, : « Le projet de l'école Boulle m'a particulièrement impressionné, par sa créativité, ses angles, très bien choisis, et la qualité remarquable de sa réalisation. Très cohérent et utile, je l'ai trouvé particulièrement juste ».

Et après ?
Lors de la soirée de remise des prix organisée à la CNIL, les lauréats ont pu rencontrer des membres du collectif Educnum et de la CNIL, la Présidente d'Universcience, la Direction du numérique pour l'éducation. Autant de bons conseils à échanger pour faire grandir ces projets et transmettre les bonnes pratiques au plus grand nombre.
« L'éducation au numérique est une responsabilité partagée qui nécessite une mobilisation générale. Les membres du collectif s'engagent à valoriser les projets retenus sur leurs supports de communication : sites Internet, réseaux sociaux.C'est le moyen pour ces étudiants d'avoir une très bonne visibilité et de pouvoir bénéficier d'une aide dans la réalisation future de leurs projets. », indique Isabelle Falque-Pierrotin, Présidente de la CNIL.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.cnil.fr/linstitution/actualite/article/article/remise-des-trophees-du-1er-concours-educnum-operation-vie-privee/

L’obligation de notification des violations de données à caractère personnel à la CNIL

L’obligation de notification des violations de données à caractère personnel à la CNIL

À l'occasion de la révision des directives « Paquet télécom » en 2009, le législateur européen a imposé aux fournisseurs de services de communications électroniques l'obligation de notifier les violations de données personnelles aux autorités nationales compétentes, et dans certains cas, aux personnes concernées.

Cette obligation de notification a été transposée en droit français à l'article 34 bis de la loi informatique et libertés. Les conditions de sa mise en œuvre ont été précisées par le décret n° 2012-436 du 30 mars 2012, ainsi que par le règlement européen n° 611/2013 du 24 juin 2013.

Dans quels cas l'article 34 bis s'applique-t-il ?
L'article 34 bis de la loi informatique et libertés s'applique lorsque plusieurs conditions sont réunies :
• condition 1 : il faut qu'un traitement de données à caractère personnel ait été mis en œuvre
• condition 2 : le traitement doit être mis en oeuvre par un fournisseur de services de communications électroniques
• condition 3 : dans le cadre de son activité de fourniture de services de communications électroniques (par exemple, lors de la fourniture de son service de téléphonie ou d'accès à d'internet)
• condition 4 : ce traitement a fait l'objet d'une violation. Selon l'article 34 bis, une violation est constituée par une destruction, une perte, une altération, une divulgation, ou un accès non autorisé à des données à caractère personnel. Elle peut se produire de manière accidentelle ou illicite, l'intention malveillante étant l'un des possibles cas de figure, mais pas le seul.

Sont, par exemple, constitutifs d'une violation :
• Une intrusion dans la base de données de gestion clientèle d'un fournisseur d'accès internet (FAI) ;
• Une faille dans la boutique en ligne d'un opérateur mobile permettant de récupérer les numéros de cartes de crédits des clients ayant commandé un nouveau téléphone associé à un forfait (car ce sont les données clients collectées en tant qu'opérateur) ;
• Un email confidentiel destiné à un client d'un FAI, diffusé par erreur à d'autres personnes ;
• La perte d'un contrat papier d'un nouveau client par un agent commercial d'un opérateur mobile dans une boutique.

Ne sont pas des violations de données personnelles au sens de l'article 34 bis :
• Toute violation ne concernant pas un traitement du FAI comme un virus informatique qui s'attaque aux PC des abonnés du FAI pour collecter des données personnelles ;
• Toute activité ne concernant pas la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public tel que le piratage du fichier des ressources humaines du FAI.

Qui doit notifier la CNIL et informer les personnes concernées par la violation ?
L'article 34 bis vise les « fournisseurs de services de communications électroniques accessibles au public ». Il s'agit des opérateurs devant être déclarés auprès de l'ARCEP (article L. 33-1 alinéa 1 du code des postes et des communications électroniques) (par exemple, les fournisseurs d'accès à internet ou de téléphonie fixe et mobile).
Les services de la société d'information, tels que les banques en ligne, les sites d'e-commerce ou les téléservices des administrations, ne sont pas concernés.

Quand et comment notifier la CNIL ?
Toute violation doit être notifiée à la CNIL, quelle que soit son niveau de gravité.
La notification doit être adressée à la CNIL dans les 24h de la constatation de la violation.
Si le fournisseur de services de communications électroniques ne peut fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, il est possible de procéder à une notification en deux temps :
Une notification initiale dans les 24 heures de la constatation de la violation ; puis
Une notification complémentaire dans le délai de 72 heures après la notification initiale.
Cette notification doit se faire par lettre remise contre signature ou via le formulaire de dépôt en ligne accessible sur le site de la CNIL, à l'aide du formulaire de notification prévu à cet effet [faire un lien vers le formulaire de notification].

Quand informer les personnes ?
L'information des personnes doit être effectuée sans retard injustifié après constat de la violation de données à caractère personnel (article 91-2 du décret).
Cependant, le fournisseur n'a pas l'obligation d'informer les personnes dans les cas suivants :
la violation n'est pas susceptible de porter atteinte aux données ou à la vie privée des personnes (un outil permettant d'évaluer le niveau de gravité d'une violation est disponible sur le site de la CNIL) ;
la violation est susceptible de porter atteinte aux données ou à la vie privée des personnes, mais le fournisseur a mis en place des mesures techniques de protection appropriées (article 91-3 du décret). Mises en place préalablement à la violation, ces mesures doivent avoir rendues les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès (voir ci-dessous).

Que sont des mesures de protection appropriées ?
Il s'agit de toute mesure technique efficace destinée à rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès. Par exemple, le fait de chiffrer les données permet de rendre les données incompréhensibles à des tiers dans la mesure où la clé de chiffrement n'a pas été compromise.
Si le fournisseur a mis en œuvre de telles mesures de protection, il doit en informer la CNIL au moment de la notification. En effet, pour que le fournisseur puisse être dispensé d'informer les personnes, la CNIL doit d'abord constater que les mesures sont appropriées et qu'elles ont été efficacement mises en œuvre.
La CNIL a deux mois pour se prononcer sur ces mesures. En cas de silence de la CNIL, elles sont considérées comme ne répondant pas aux exigences de l'article 34 de la loi informatique et libertés et le fournisseur doit avertir les personnes.

La CNIL peut-elle imposer au fournisseur d'informer les personnes ?
Oui, la CNIL peut imposer au fournisseur d'informer les personnes si elle constate que la violation porte atteinte aux données ou à la vie privée des personnes, que les mesures de protection mises ne place n'étaient pas appropriées ou que les personnes n'ont pas été ou ont été mal informé.

Comment informer les personnes ?
L'information des personnes doit être faite par tout moyen permettant d'apporter la preuve de l'accomplissement de cette formalité (par courrier électronique, par exemple). Cette information doit contenir les éléments suivants :
• le nom du fournisseur ;
• l'identité et les coordonnées du correspondant informatique et libertés ou d'un point de contact auprès duquel les personnes peuvent obtenir des informations supplémentaires ;
• le résumé de l'incident à l'origine de la violation ;
• la date estimée de l'incident ;
• la nature et la teneur des données concernées ;
• les conséquences vraisemblables de la violation pour la personne ;
• les circonstances de la violation ;
• les mesures prises pour remédier à la violation ;
• les mesures recommandées par le fournisseur pour atténuer les préjudices potentiels.
En outre, cette information doit être rédigée dans une langue claire et aisément compréhensible. Elle ne doit pas être utilisée comme un moyen de promouvoir ou d'annoncer de nouveaux services ou être associée à d'autres informations (être mentionnée sur la facture adressée aux personnes concernées, par exemple).

Quels sont les risques pris par le fournisseur qui ne notifierait pas ?
Le fournisseur encourt des sanctions pénales car le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la CNIL ou à l'intéressé est puni de cinq ans d'emprisonnement et de 300 000 € d'amende (article 226-17-1 du code pénal).
En outre, tout manquement à la loi informatique et libertés est passible de sanctions administratives, notamment financières pouvant aller jusqu'à 300 000 €.

En cas de violations, le fournisseur a-t-il d'autres obligations que la notification ?
Oui, il doit tenir à jour un inventaire des violations qui doit notamment contenir les modalités de la violation (ce qui s'est passé), l'effet de la violation (les conséquences) et les mesures prises pour remédier à la violation (les actions correctives mises en œuvre).
Ce recensement des violations peut être réalisé sous format papier ou numérique, et doit être conservé à la disposition de la CNIL.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.cnil.fr/linstitution/actualite/article/article/la-notification-des-violations-de-donnees-a-caractere-personnel

---

Que risquez-vous si vous égarez une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

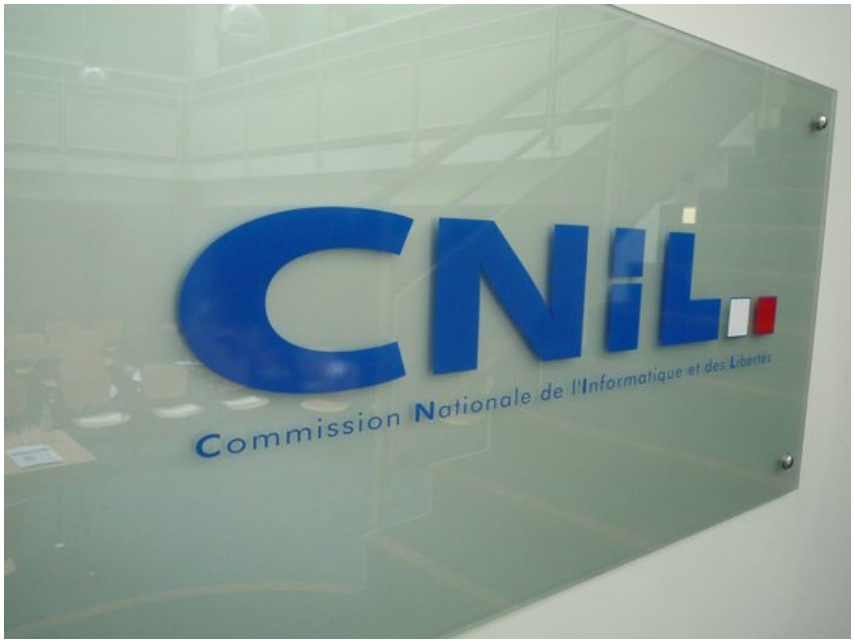
Que risquez-vous si vous égarez une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

Si votre système informatique se fait pirater (comme l'ont été les sites Internet de SONY, Orange, Google, Bercy, le ministère des Finances…), les auteurs de l'attaque ne sont pas les seuls à être inquiétés d'une telle fuite. Les responsables du traitement peuvent en effet avoir à fournir quelques explications à la CNIL. Même sanction, si vous perdez votre clé USB, disque dur externe ou pire, votre ordinateur portable. Et pour cause, si vous manipulez des données qui permettent d'identifier une personne, communément appelées des données personnelles), vous êtes tenus à une série d'obligations de sécurité afin d'éviter la violation de données à caractère personnel (destruction, perte, altération, divulgation, accès non autorisé).
L'article 34 bis de la loi Informatique et Libertés les oblige par exemple à avertir sans délai la CNIL et à tenir à jour un registre des incidents. En principe, les particuliers, victimes collatérales de cette faille, doivent également être informés sans délai, sauf si la CNIL « a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation ». En clair, pas d'alerte direct des clients si les rustines ont été correctement appliquées.
Plus globalement, l'article 34 de la loi Informatique et Libertés impose au responsable d'un traitement de prendre toutes précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Évidemment, cette protection diffère selon la nature des données et des risques présentés par le traitement.
Enfin, selon l'article 226-17 du Code pénal, le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Etonnant non ?

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.nextinpact.com/news/91600-un-partenaire-tf1-pirate-quelles-consequences-juridiques.htm
Extrait de Marc Rees adapté par Denis JACOPINI

La Cnil lance un nouveau label sur la gestion des données



La Cnil lance un nouveau label sur la gestion des données

Face à la prolifération des données qu'une entreprise a à gérer et à la complexité réglementaire qui l'accompagne, la Cnil lance un nouveau label visant à prouver la conformité de sa gouvernance.

Garantir à ses clients que l'on est conforme aux bonnes pratiques de la Cnil en matière de gestion des données personnelles, c'est l'objet de ce nouveau label « Gouvernance Informatique et Libertés » dévoilé par la Commission. Après les labels « formation », « procédure d'audit » et « coffre-fort numérique », la Cnil veut maintenant donner au Correspondant Informatique et Libertés (Cil) un autre moyen d'améliorer la gestion.
Pour rappel, le Cil est depuis 2005 la personne intermédiaire entre une entreprise et la Cnil. Du coup, ce nouveau référentiel s'adressera forcément aux organisations possédant un tel référent (plus de 10 000 à ce jour). La création de ce nouveau label est partie du constat du régulateur que les entreprises et organismes publics avaient de plus en plus besoin « d'identifier clairement les procédures à mettre en place pour une bonne gestion des données personnelles ». Pour y prétendre, 25 exigences (.rtf) ont été définies par la Cnil.
Celles-ci sont organisées en trois thématiques : l'organisation interne liée à la protection des données, la méthode de vérification de la conformité des traitements à la loi Informatique et Libertés et la gestion des réclamations et incidents. Pour le régulateur, ce label témoignera « de la volonté de l'organisme d'innover et de traiter les données personnelles de manière responsable » et constituera donc un atour pour ses clients.

Tous les organismes, publics ou privés ayant désigné un correspondant informatique et libertés peuvent prétendre à ce label.
Téléchargez le dossier de candidature
Une fois complété, envoyez le dossier
soit par le biais du formulaire de dépôt en ligne
soit par courrier postal (CNIL, 8 rue Vivienne, CS30223, 75083 paris Cedex 02)

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://pro.clubic.com/legislation-loi-internet/donnees-personnelles/actualite-749887-cnil-gestion-donnees-personnelles-entreprise.html

---

Que risquez-vous vous égarez

une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

Que risquez-vous vous égarez une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

Si votre système informatique se fait pirater (comme l'ont été les sites Internet de SONY, Orange, Google, Bercy, le ministère des Finances…), les auteurs de l'attaque ne sont pas les seuls à être inquiétés d'une telle fuite. Les responsables du traitement peuvent en effet avoir à fournir quelques explications à la CNIL. Même sanction, si vous perdez votre clé USB, disque dur externe ou pire, votre ordinateur portable. Et pour cause, si vous manipulez des données qui permettent d'identifier une personne, communément appelées des données personnelles), vous êtes tenus à une série d'obligations de sécurité afin d'éviter la violation de données à caractère personnel (destruction, perte, altération, divulgation, accès non autorisé).

L'article 34 bis de la loi Informatique et Libertés les oblige par exemple à avertir sans délai la CNIL et à tenir à jour un registre des incidents. En principe, les particuliers, victimes collatérales de cette faille, doivent également être informés sans délai, sauf si la CNIL « a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation ». En clair, pas d'alerte direct des clients si les rustines ont été correctement appliquées.
Plus globalement, l'article 34 de la loi Informatique et Libertés impose au responsable d'un traitement de prendre toutes précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Évidemment, cette protection diffère selon la nature des données et des risques présentés par le traitement.
Enfin, selon l'article 226-17 du Code pénal, le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Etonnant non ?

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.nextinpact.com/news/91600-un-partenaire-tf1-pirate-quelles-consequences-juridiques.htm
Extrait de Marc Rees adapté par Denis JACOPINI

Un partenaire de TF1 piraté, quelles conséquences juridiques ? – Next INpact

Que risquez-vous vous égarez une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

Si votre système informatique se fait pirater (comme l'ont été les sites Internet de SONY, Orange, Google, Bercy, le ministère des Finances…), les auteurs de l'attaque ne sont pas les seuls à être inquiétés d'une telle fuite. Les responsables du traitement peuvent en effet avoir à fournir quelques explications à la CNIL. Même sanction, si vous perdez votre clé USB, disque dur externe ou pire, votre ordinateur portable. Et pour cause, si vous manipulez des données qui permettent d'identifier une personne, communément appelées des données personnelles), vous êtes tenus à une série d'obligations de sécurité afin d'éviter la violation de données à caractère personnel (destruction, perte, altération, divulgation, accès non autorisé).

L'article 34 bis de la loi Informatique et Libertés les oblige par exemple à avertir sans délai la CNIL et à tenir à jour un registre des incidents. En principe, les particuliers, victimes collatérales de cette faille, doivent également être informés sans délai, sauf si la CNIL « a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation ». En clair, pas d'alerte direct des clients si les rustines ont été correctement appliquées.
Plus globalement, l'article 34 de la loi Informatique et Libertés impose au responsable d'un traitement de prendre toutes précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Évidemment, cette protection diffère selon la nature des données et des risques présentés par le traitement.
Enfin, selon l'article 226-17 du Code pénal, le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Etonnant non ?

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.nextinpact.com/news/91600-un-partenaire-tf1-pirate-quelles-consequences-juridiques.htm
Extrait de Marc Rees adapté par Denis JACOPINI

Enregistrement des appels téléphoniques au travail – La CNIL simplifie les règles

	Enregistrement des appels téléphoniques au travail – La CNIL simplifie les règles

La CNIL a fait publier au Journal Officiel une délibération créant une norme simplifiée pour autoriser les entreprises et les administrations à enregistrer les conversations téléphoniques des employés sur le lieu de travail.

Comme l'y autorise l'article 24 de la loi du 6 janvier 1978, la CNIL a publié une « norme simplifiée » qui permet d'alléger les formalités administratives pour être autorisé à procéder à l'écoute et l'enregistrement des conversations téléphoniques du personnel sur le lieu de travail. La norme, qui vaut autorisation pour quiconque déclare s'y conformer, a été publiée ce mardi au Journal Officiel, en tant que délibération n° 2014-474 du 27 novembre 2014.
Elle autorise les entreprises et les administrations à écouter et enregistrer les conversations téléphoniques des agents et employés, avec toutefois un certain nombre de réserves. Notamment :
Les écoutes et enregistrements doivent être « ponctuels » et donc ne peuvent pas avoir de caractère « permanent ou systématique », y compris pour les salariés qui seraient en période d'essai. Toutefois la CNIL se garde de fixer un critère chiffré, que ce soit en quantité brute ou en proportion d'appels enregistrables ;

Il n'est pas autorisé de croiser les enregistrements avec des données provenant d'une capture d'écran du poste informatique de l'employé ;

Les enregistrements doivent uniquement servir à la formation des employés, leur évaluation ou « l'amélioration de la qualité du service » ;

L'enregistrement vidéo est proscrit dans le cadre de la norme simplifiée (c'est-à-dire il faut solliciter une autorisation complémentaire) ;

Les employés et leurs interlocuteurs doivent être informés de la possibilité d'enregistrement, et d'une série d'informations complémentaires (finalité, catégories de données traitées, destinataires, transfert hors UE le cas échéant, droit d'accès…).

Les enregistrements doivent être effacés au maximum 6 mois après leur collecte, et conservés avec « toutes précautions utiles pour préserver la sécurité des données », notamment d'identification des personnes autorisées à y avoir accès.

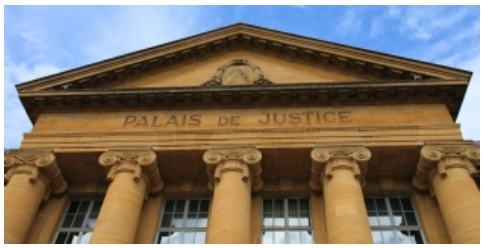
En outre, la CNIL précise que la norme simplifiée s'applique également aux « documents d'analyse, tels que les comptes-rendus ou les grilles d'analyse réalisés dans le cadre des écoutes et des enregistrements ». Elle précise que les données collectées dans ce cadre doivent être « adéquates, pertinentes et non excessives » au regard des finalités définies, et qu'elles ne peuvent porter que sur les données identifiant l'employé et l'évaluateur, les informations techniques de l'appel (date, heure, durée), et l'évaluation professionnelle correspondante.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.numerama.com/magazine/31780-la-cnil-simplifie-l-enregistrement-des-appels-telephoniques-au-travail.html
Par Guillaume Champeau

Attention à bien déclarer à la CNIL le traitement de vos

fichiers clients, salariés, patients…



Attention à bien déclarer à la CNIL le traitement de vos fichiers clients, salariés, patients…

S'il n'a pas été déclaré à la CNIL, votre traitement de données personnelles est illicite. Tout comme les éléments qu'il vous fournira pour justifier le licenciement d'un salarié.

Tout traitement de données personnelles est illicite s'il n'a pas été préalablement et correctement déclaré à la Cnil (sauf si ces moyens de traitement sont couverts par l'une des 19 dispenses prononcées par la commission). Conséquence : la chambre sociale de la Cour de Cassation a cassé l'arrêt de la Cour d'Appel de Douai, qui avait approuvé le licenciement d'une salariée pour cause réelle et sérieuse alors que ce dernier était fondé uniquement sur le système de contrôle du nombre et du contenu des courriels des salariés mis en place par la société.

Cette dernière n'ayant pas déclaré ce système (qui constitue un traitement de données personnelles) auprès de la Cnil, ce système était illégal et la société ne pouvait donc pas utiliser les preuves qu'elle s'était ainsi constituées. Il convient de rappeler que la déclaration auprès de la Cnil n'est pas la seule condition de la légalité d'un traitement de données personnelles, cette légalité étant également conditionnée, en particulier, par l'information préalable des personnes concernées.

Non respect de la Loi Informatique et Libertés du 6 janvier 1978 :
Peines encourues : 5 ans de prison et 300 000 euros d'amende
Articles sur le même thème :
Se mettre en conformité avec la CNIL – Oui mais comment ?
Est-ce que votre site Internet est en règle avec la CNIL ?

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.chefdentreprise.com/Thematique/management-rh-1026/droit-social-10119/Breves/Jurisprudence-Attention-declarer-CnIL-votre-systeme-controle-donnees-personnelles-248669.htm

---

Wifi en libre accès : conseils pour ne pas se faire épingler par la Cnil pour « des manquements récurrents »

Wifi en accès libre : conseils pour ne pas se faire épingler par la Cnil pour « des manquements récurrents »

La Commission nationale de l'informatique et des libertés (Cnil) a de bons côtés, parmi lesquels sa volonté inébranlable de garder la pêche. Chaque jour que Dieu fait, elle constate des entorses aux règles qu'elle est censée faire respecter, mais ne se décourage pas.

Nouvel exemple : l'autorité administrative indépendante a contrôlé des points où internet est disponible en libre accès – restaurants, hôtels, bibliothèques – via le wifi ou des postes informatiques dédiés. Sans surprise, elle a découvert « des manquements récurrents » :
• de nombreux opérateurs « conservent des données portant sur le contenu des correspondances échangées ou des informations consultées (URL) alors qu'ils ne sont pas autorisés à le faire » ;
• ils ne doivent conserver que les données de connexion, pendant un an. Or, la plupart les gardent indéfiniment ;
• les utilisateurs sont mal informés ;
• plusieurs opérateurs utilisent « des outils de surveillance » des postes informatiques comme la « prise en main à distance » et le « contrôle de l'historique de navigation ». C'est-à-dire qu'ils ont accès, de fait à des données sensibles : « identifiants-mots de passe, numéros de compte bancaire, etc ». La Cnil aimerait qu'ils arrêtent.
• les réseaux wifi, sans chiffrement et facilement accessibles, sont de vraies passoires. Il n'est pas difficile d'en prendre le contrôle.
Plutôt que de paniquer devant tant d'amateurisme, la Cnil garde le cap et donne cinq conseils pour améliorer les choses.

Au restaurant, à l'hôtel ou dans les bibliothèques, il est souvent possible d'utiliser un réseau internet wi-fi ou des postes informatiques en libre accès.
La CNIL a décidé d'intégrer dans son programme annuel des contrôles la thématique de l'internet en libre accès. Elle a effectué plusieurs contrôles des modalités de mise en œuvre de ce type de service auprès d'organismes privés et publics.

Lors de ces contrôles, l'attention de la CNIL a principalement porté sur :
• le type de données collectées,
• leur conservation,
• le niveau d'information des utilisateurs
• la qualité des mesures de sécurité qui y sont associées.

Plusieurs manquements récurrents ont été identifiés lors de ces contrôles. Au vu de ces constations, la CNIL rappelle aux fournisseurs de services d'internet en libre accès les mesures à adopter pour se mettre en conformité.

1. Conserver seulement les données de trafic
Les organismes qui mettent à disposition du public un service de libre accès à internet (postes informatiques, wi-fi, etc.) sont considérés comme opérateurs de communications électroniques (OCE) et sont soumis aux obligations prévues à l'article L. 34-1 du code des postes et des communications électroniques (CPCE). A ce titre, ils doivent conserver les données de trafic répondant aux » besoins de la recherche, de la constatation et de la poursuite des infractions pénales » et destinées aux autorités légalement habilitées.
La CNIL a constaté lors des contrôles que de nombreux opérateurs de communication électronique conservaient des données portant sur le contenu des correspondances échangées ou des informations consultées (URLs) alors qu'ils ne sont pas autorisés à le faire (article L. 34-1 VI du CPCE consultable sur http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465770&dateTexte=&categorieLien=cid).
Les fournisseurs de service ne doivent pas collecter de telles données et supprimer celles qui auraient été conservées.

2. Définir une durée de conservation des données limitée et proportionnée
La plupart des fournisseurs de service conservent les données issues des journaux de connexion sans qu'aucune durée de conservation n'ait été définie.
Or, les données de trafic doivent être conservées pendant 1 an à compter du jour de leur enregistrement (Article R. 10-13 du Code des postes et des communications électroniques consultable sur http://legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006466369&cidTexte=LEGITEXT000006070987&dateTexte=20110909&oldAction=rechCodeArticle)
Les autres données collectées dans le cadre de l'offre d'internet en libre accès, telles que les informations d'abonnement, etc. doivent être supprimées régulièrement (article 6-5° de la loi n°78-17 du 6 janvier 1978 modifiée consultable sur http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/#Article6) lorsqu'elles ne sont plus nécessaires (désinscription ou inutilisation prolongée de l'abonnement).

3. Fournir une information complète sur les traitements de données :
Les contrôleurs de la CNIL ont observé que l'information fournie aux utilisateurs des services d'internet en libre accès, ne s'avérait pas toujours satisfaisante, voire inexistante.
Les opérateurs de communication électronique doivent délivrer une information aux utilisateurs de leur service sur les modalités de traitement de leurs données (article 32 de la loi n°78-17 du 6 janvier 1978 modifiée). Le support de cette information doit être le formulaire d'inscription au service. A défaut, l'information doit être fournie par voie d'affichage, dans une charte informatique, etc. (Voir les modèles de mention d'information sur http://www.cnil.fr/vos-obligations/informations-legales/).
Par ailleurs, les opérateurs de communication électronique doivent prévoir des procédures de gestion des demandes d'accès, de rectification et de suppression des données par leurs utilisateurs (art. 38 à 40 de la loi n°78-17 du 6 janvier 1978 modifiée).

4. Veiller à la conformité des outils utilisés, notamment aux outils de surveillance :
Plusieurs opérateurs de communication électronique contrôlés utilisaient des outils de surveillance afin d'assurer la sécurité des postes informatiques, la gestion des tarifications, les impressions, etc.
L'utilisation de tels outils (consultation ou prise en main à distance, contrôle de l'historique de la navigation, etc.) est susceptible de donner accès à un grand nombre d'informations excessives au regard de la finalité pour laquelle elles sont collectées (identifiants-mots de passe, numéros de compte bancaire, etc). Le recours à de tels outils doit être évité ou un paramétrage limité doit être mis en place.

5. Assurer la confidentialité et la sécurité des données :
Plusieurs lacunes en termes de sécurité et de confidentialité ont été révélées lors des contrôles :
• L'absence de chiffrement des réseaux wi-fi ;
• L'accessibilité du BIOS (absence ou faiblesse du mot de passe) permettant de modifier la configuration basique du système ;
• La possibilité de prendre le contrôle de la machine en démarrant un système d'exploitation depuis une clé USB ; etc.
Pour y remédier, les opérateurs de communication électronique doivent inclure une clause relative à la sécurité des données dans le contrat conclu avec le prestataire réseaux (voir le modèle de clause de confidentialité sur http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/sous-traitance-modeles-de-clauses-de-confidentialite).
Par ailleurs, ils doivent adopter des mesures de sécurité afin de (voir les guides sur » La sécurité des données personnelles » sur http://www.cnil.fr/documentation/guides/) .

Au travers de missions de mise en conformité ou de formation d'un futur correspondant CNIL (Correspondant Informatique et Libertés dit aussi CIL), Denis JACOPINI se charge de mettre en conformité votre établissement avec la Loi Informatique et Libertés auprès de la CNIL.
Vous souhaitez vous mettre en conformité avec la CNIL, contactez-nous

---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://rue89.nouvelobs.com/2014/12/22/wifi-libre-acces-cnil-epingle-manquements-recurrents-256697