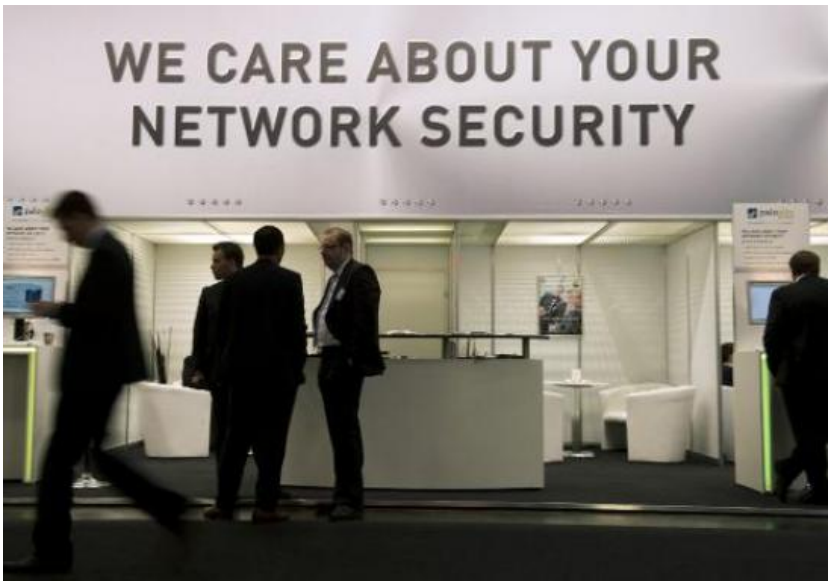
La justice néerlandaise annule une loi sur les données personnelles | Le Net Expert Informatique



La justice néerlandaise annule une loi sur les données personnelles

La justice néerlandaise a annulé mercredi une loi exigeant le stockage de données personnelles, assurant que bien qu'utile à la lutte contre le crime, le texte violait la vie privée des utilisateurs des réseaux téléphoniques et d'internet.

« Les juges ont estimé que le stockage de données était nécessaire et efficace pour combattre le crime, mais la législation néerlandaise est contraire aux droits des personnes à une vie privée et à la protection de leurs données personnelles », a indiqué le tribunal de La Haye dans un communiqué.
« La loi est donc contraire à la Charte des droits fondamentaux de l'Union européenne », a ajouté le tribunal.
Sept organisations, dont l'organisation de défense de la vie privée Privacy First et l'Association néerlandaise des Journalistes, avaient entamé une action contre l?État le mois dernier.
Cette décision des juges intervient environ un an après une décision de la justice européenne, qui avait imposé en avril 2014 une révision de la législation sur la conservation des données personnelles, la jugeant « disproportionnée » malgré son utilité dans la lutte contre le terrorisme.
La directive en question datait de 2006 et exigeait des opérateurs de télécoms et des fournisseurs d'accès internet de stocker les données des communications téléphoniques ou de courriels pendant six mois à deux ans.
Étaient donc conservées les métadonnées desdites communications, comme l'heure, la date, la durée et la destination, mais pas leur teneur.
Ces données pouvaient ensuite être consultées par les services de renseignement ou la police.
« Les droits à une vie privée des citoyens néerlandais ont été violés en masse par cette surveillance », a affirmé Vincent Boehre, le directeur des opérations de Privacy First, cité dans un communiqué publié sur le site internet de l'organisation.
Privacy First « lutte pour une société dans laquelle des civils innocents ne doivent pas se sentir comme s'ils étaient constamment surveillés », a-t-il ajouté, soulignant que ce jugement est « une étape importante dans cette direction ».

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

Source : http://www.leparisien.fr/high-tech/la-justice-neerlandaise-annule-une-loi-sur-les-donnees-personnelles-11-03-2015-4595081.php

---

Accord pour faciliter les plaintes transfrontalières | Le Net Expert Informatique

Accord pour faciliter les plaintes transfrontalières

Les Etats membres de l'Union européenne se sont accordés ce vendredi à Bruxelles sur le principe de permettre aux entreprises et aux citoyens le dépôt, au sein de leur Etat national, d'une plainte en matière de protection de la vie privée contre une entreprise du web établie dans un autre Etat.

Ce guichet unique («one-stop-shop») serait compétent pour veiller à l'application des règles pour les transferts transfrontaliers de données personnelles collectées dans plusieurs pays de l'UE par des entrepri1ses ou des plate-formes internet comme Amazon, Google, Facebook.
Les plaignants auront la possibilité de saisir leurs autorités nationales, comme la Commission de la protection de la vie privée en Belgique, en cas de litige.
Le but est d'obtenir une procédure plus rapide, des coûts et une charge administrative moindres ainsi qu'une sécurité juridique accrue.
Le secrétaire d'Etat belge en charge de la protection de la vie privée, Bart Tommelein, ne voit que des avantages au principe du guichet unique, mais reconnaît sa complexité. «Nous devrons activer ce système avant de voir par la suite comment l'améliorer et le simplifier», a-t-il commenté.
Un accord global sur la législation sur la protection des données personnelles est toutefois encore loin d'être définitif.
Les ministres européens de la Justice ont donc décidé de se réunir en «conclave» le 15 juin à Luxembourg afin de conclure un accord.
Les discussions sont engagées depuis février 2012, mais elles ont longtemps piétiné. Onze chapitres sont ouverts, et six ont fait l'objet d'un accord de principe, dont celui portant sur la création d'un «guichet unique».
Sur les cinq restant en discussion, on relève celui concernant les droits des personnes, avec le droit d'accès aux données collectées, le droit de les faire rectifier et le droit à l'oubli avec la possibilité «de faire effacer les informations mises en ligne avec insouciance par les mineurs».

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

Source : http://www.lavenir.net/cnt/dmf20150313_00616117

L’externalisation, pourquoi et comment ? | Le Net Expert Informatique

L’externalisation, pourquoi et comment ?

L'externalisation (ou sous traitance) se développe de plus en plus en France, quels sont les avantages pour les professionnels du droit à avoir recours à ce type de service, et dans quelles conditions peut-elle être mise en place ?

L'externalisation c'est l'Action pour une entreprise de confier une partie de ses activités à des partenaires extérieurs.(Larousse). Aujourd'hui sous traiter se développe de plus en plus en France. Mais comment en tant que professionnel pouvez-vous inclure cette prestation extérieure dans la gestion quotidienne de votre activité ? Quelles taches peuvent être sous traitées ? Par qui ? Quid de la confidentialité des données transmises ? Quels sont les bénéfices et avantages ?

Des bénéfices et des avantages pour les professionnels
Le fait de confier des taches récurrentes et chronophages à une entreprise extérieure permet de réduire automatiquement vos frais de gestion, et vos charges liées au personnel. Des économies vous permettant une meilleure gestion de votre activité (réinvestissement, augmentation du budget communication ou publicitaire…).
De plus, comme un assistant, votre prestataire extérieur connait vos besoins et s'adapte. Il est possible de lui dicter vos conditions, et de travailler avec lui suivant votre fonctionnement.

Quelles taches peuvent être sous traitées ?
Autant de questions que les professionnels se posent avant de « sauter le pas ». Il existe des agences ou des cabinets spécialisés en expertise comptable, pour la gestion de la paie et des ressources humaines. Il est également possible d'externaliser une partie de son secrétariat, ou de sa permanence téléphonique.
Il suffit de déterminer au préalable un besoin : Aujourd'hui je ne peux plus répondre à mon standard téléphonique, ou je n'ai pas le temps de saisir mes courriers ou mes actes, j'aimerai trouver un expert comptable pour la gestion de ma comptabilité…

Comment inclure la prestation dans ma gestion quotidienne, et par qui sera t-elle réalisée ?
Votre prestataire est là pour vous aider à mettre en place la prestation et sa gestion au quotidien. Il est un professionnel qualifié et diplômé. N'hésitez pas à demander la qualification de la personne effectuant les tâches à l'entreprise. La prise en charge de la permanence téléphonique ou l'envoi par email d'un courrier à taper ou d'un fichier à retranscrire par email, autant de solutions qui peuvent être trouvées pour vous décharger de certaines taches.

Et la confidentalité des données ?
Votre prestataire, tenu au secret professionnel se doit de vous garantir la confidentialité des données en n'effectuant aucune sauvegarde de fichiers transmis. N'hésitez pas à faire ajouter cette mention lors du devis signé entre les deux parties.
L'externalisation ou sous traitance ne doit pas être vue comme une contrainte, mais plutôt comme une solution de « facilitateur » du quotidien. Elle peut être utilisée ponctuellement ou pour répondre à un besoin régulier. Un bon moyen de recentrer le travail de vous et/ou collaborateurs sur l'essentiel de leurs taches et missions quotidien et de se concentrer sur l'essentiel de l'activité.

ATTENTION :
Ce n'est pas parce que vous bénéficiez des services d'un prestataire que ceci vous exempt de déclaration à la CNIL des traitements de données à caractères personnel qui seront manipulées.
Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Vous trouverez plus d'information sur le site de la cnil (www.cnil.fr) ou, étant correspondant CNIL local, dans notre rubrique Protection des données personnelles.

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 protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.village-justice.com/articles/externalisation-pourquoi-comment,19173.html
Par Mme Pollet, responsable de l'entreprise APSAEE, spécialisée dans la sous traitance du Secrétariat Juridique : Permanence téléphonique et Retranscription audio.

Les experts de la sécurité se penchent sur la Watch d'Apple | Le Net Expert Informatique

Les experts de la sécurité se penchent sur la Watch d'Apple

La firme de Cupertino a donc lancé officiellement sa montre connectée, la Watch, le 9 mars 2015 hier soir. Tout a été dit sur ce gadget déclinable en plusieurs versions dont une luxueuse au prix stratosphérique de 11 000 euros. Mais cette annonce a aiguisé la curiosité des experts en sécurité qui se sont penchés sur les faiblesses de la tocante numérique.

Nos confrères de The Register ont interrogé plusieurs spécialistes de la sécurité sur ce sujet. Ainsi, Ken Westin, chercheur chez Tripwire a indiqué que « le fait que le dispositif soit à la fois WiFi et Bluetooth va faciliter le développement des fonctionnalités supplémentaires à la montre et de s'interopérer avec d'autres équipements. Mais cela va également augmenter la surface d'attaque de l'appareil ». Pour lui, il ne fait aucun doute que « les chercheurs et les hackers ont été émoustillés pour trouver de nouvelles vulnérabilités et s'appuyer sur des attaques existantes qui profitent des faiblesses du WiFi et du Bluetooth ».

Problème de confidentialité des données
Un autre aspect de sécurité selon l'expert réside dans la confidentialité des données. « Avec ces connectivités, il sera intéressant de voir comment les données peuvent être utilisées pour suivre les personnes dans espaces physiques. Cela peut avoir un impact pour un cyberattaquant, tout comme pour des campagnes publicitaires trop ciblés ». L'arrivée d'applications tierces n'est pas faite pour rassurer le spécialiste qui y voit un risque supplémentaire pour la sécurité et la vie privée.

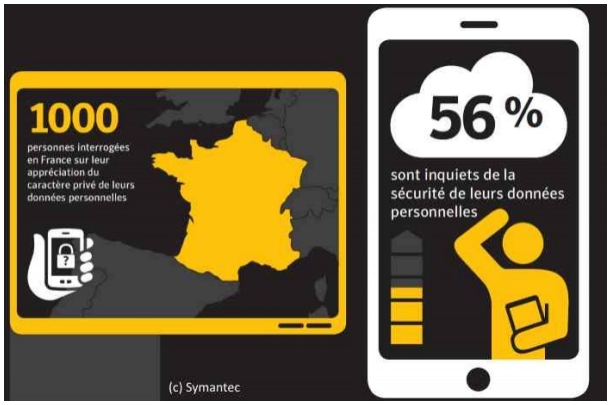
La fraude au paiement
En disposant d'une capacité NFC, l'Apple Watch peut servir pour le paiement mobile. Les risques de fraudes existent donc. Une récente étude de Drop Labs montre que le niveau de fraude sur les paiements avec Apple Pay est de 6% contre 1% en moyenne pour les transactions par carte bancaire. Pour la défense d'Apple, le problème vient surtout d'un niveau d'authentification faible de la part des banques. Une affaire récente a démontré ce risque. Certains spécialistes s'interrogent sur la fiabilité de la technologie NFC avec la capacité de la contourner.

Une révision des politiques de BYOD ?
Phil Barnett, directeur général EMEA de Good Technology, préfère souligner les menaces que les montres connectées et plus généralement les « wearables technology » impliquent dans le monde du travail. Elles s'inscrivent dans les politiques de BYOD (Bring Your Own Device) qui selon lui doivent être révisées. « Le BYOD a déjà connu les smartphones et des tablettes, les accessoires connectés arrivent comme les prochains véhicules de la donnée. Ils représentent une immense opportunité pour la productivité, mais ils nécessitent avant leur arrivée en entreprise de les sécuriser. »
Cela passe pour lui par plusieurs axes : « Chiffrement des données transitant sur le Bluetooth et la conteneurisation des données de l'entreprise. Par ailleurs, un contrôle plus granulaire des politiques de sécurité devrait permettre de trouver un équilibre entre risques et productivité. » A condition qu'il n'y ait pas de défaut dans la cuirasse, comme le montre la faille Freak qui affaiblissait le chiffrement des navigateurs Apple et Android. La firme de Cupertino vient d'ailleurs de publier iOS 8.2 qui règle ce problème.

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

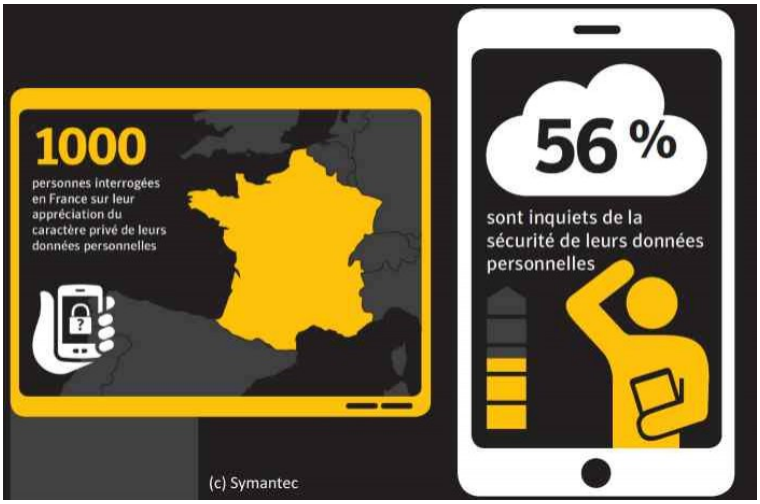
Source : http://www.silicon.fr/les-experts-de-la-securite-se-penchent-sur-la-watch-dapple-110567.html

88% des consommateurs font de la sécurité des données personnelles un élément clé de l’acte d’achat | Le Net Expert Informatique



88% des consommateurs font de la sécurité des données personnelles un élément clé de l’acte d’achat

Selon l'étude « State of Privacy » de Symantec, les consommateurs n'accordent que peu de confiance aux entreprises et administrations pour gérer leurs données personnelles. Au point de mentir.88% des consommateurs font de la sécurité des données personnelles un élément clé de l'acte d'achat, devant la qualité des produits ou le service client. Ce résultat frappant est issu d'une étude réalisée par Symantec auprès de 7000 consommateurs européens. S'il est évident que la sécurité d'un numéro de carte bancaire est un élément clé de l'achat sur un site e-commerce, la défiance des consommateurs va bien au delà. Ainsi, seulement 19% des Européens font confiance au secteur de la distribution pour la protection des données personnelles.
La confiance la plus élevée va aux hôpitaux (71% de confiance) devant les banques (62%) et l'Etat (37%). Les réseaux sociaux sont en queue de peloton avec un petit 8%. D'une manière générale, l'inquiétude à propos des données personnelles concerne 56% des consommateurs. Et 59% ont déjà eu une mauvaise expérience au sujet de leurs données personnelles.



Mentir pour se protéger
Face à la défiance générale, les consommateurs n'hésitent pas à mentir pour se protéger. Un répondant sur trois a avoué avoir donné de fausses informations en ligne. Le comportement se développe surtout chez les jeunes : 48% des 18-24 ans ont ainsi déjà menti. Mais un petit tiers accepte de laisser une adresse mail en échange d'avantages. 57% hésitent à laisser des informations personnelles à l'occasion d'un achat. Mais moins d'un sur cinq lisent les conditions d'utilisations des données avant d'n déposer.
La valeur des données est désormais bien prise en compte. 24% des répondants jugent que leurs données personnelles ont une valeur supérieure à 10 000 euros.

Vers un rôle accru de l'Etat
Qui doit agir pour mieux protéger les données personnelles ? Les résultats sont partagés. 36% des Européens et 37% des Français jugent que c'est à l'Etat d'agir avec plus de sévérité et d'efficacité. 30% des Européens et 36% des Français jugent que c'est aux entreprises avant tout d'oeuvrer pour que les données soient mieux protégées. Enfin, 33% des Européens mais seulement 27% des Français estiment que c'est de la responsabilité des individus eux-mêmes. Autrement dit : les Français sont les plus enclins à se déresponsabiliser au niveau individuel de ce qu'ils font eux-mêmes de leurs propres données personnelles.

Expert Informatique 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 protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.cio-online.com/actualites/lire-donnees-personnelles%C2%A0-l-etat-de-defiance-7435.html
Par Franck Salien, Journaliste

Sur les réseaux sociaux, il y aura bientôt plus de morts que de vivants | Le Net Expert Informatique

(Photo : Dado Ruvic/archives Reuters)	**Sur les réseaux sociaux, il y aura bientôt plus de morts que de vivants**

Un utilisateur sur cent de Facebook est décédé. Comment est prise en compte la mort sur Internet ? La Commission nationale de l'informatique et des libertés lance le débat.

« Dans quelles conditions les héritiers peuvent-ils récupérer les données d'un défunt ? », « Comment résoudre les conflits entre héritiers qui n'ont pas toujours la même perception de la volonté post-mortem du défunt ? » Autant de questions délicates, posées de plus en plus régulièrement à la Cnil (Commission nationale de l'informatique et des libertés) dans ses échanges avec les internautes.
Ces interrogations risquent de se poser encore plus souvent dans les années à venir. Car à terme, si la loi n'évolue pas, il pourrait y avoir sur les réseaux sociaux plus de morts que de vivants…

La mort est-elle suffisamment prise en compte sur Internet ? La Commission nationale de l'informatique et des libertés (Cnil) est régulièrement confrontée à des questionnements d'héritiers concernant le décès d'un proche et la gestion de sa vie numérique. Le débat sur « la mort numérique » est lancé.

« Dans quelles conditions les héritiers peuvent-ils récupérer les données d'un défunt ? », « Si rien n'est prévu dans les conditions générales d'utilisation des sites, quels sont les héritiers qui pourront demander la mise à jour ou la suppression des données ? », « Comment résoudre les conflits entre héritiers qui n'ont pas toujours la même perception de la volonté post-mortem du défunt ? » Autant de questions délicates, posées de plus en plus régulièrement à la Cnil (Commission nationale de l'informatique et des libertés) dans ses échanges avec les internautes.

Ces interrogations risquent de se poser encore plus souvent dans les années à venir. Car à terme, si la loi n'évolue pas, il pourrait y avoir sur les réseaux sociaux plus de morts que de vivants !

Sur Facebook, un mort sur cent
Actuellement, un utilisateur sur cent de Facebook est décédé. Le réseau social ne peut supprimer lui-même les comptes, en l'absence de demande des proches ou familles : comment peut-il savoir si l'utilisateur est décédé ou tout simplement inactif ? De ce contexte a émergé le concept de « mort numérique », à la fois porteur d'interrogations juridiques et sociétales.

La Cnil ayant pour rôle de contrôler la protection des données personnelles ainsi que de veiller à ce que le développement des nouvelles technologies ne porte atteinte « ni à l'identité humaine ni aux droits de l'homme, ni à la vie privée ni aux libertés individuelles ou publiques », s'est penchée sur le sujet en fin d'année 2014, afin d'ouvrir un débat sur les enjeux de la mort numérique.

Référencé à vie ?
Actuellement, si la personne concernée par le décès n'a pas programmé l'effacement de ses données, un profil numérique continue de vivre après la mort. Il reste visible sur la toile et référencé sur les moteurs de recherche. L'objectif de la Cnil est alors de savoir comment concilier le droit à l'oubli numérique et les possibilités d'atteindre l'éternité numérique offerte par la vie en ligne.

Au regard de la loi Informatique et libertés, les héritiers d'une personne décédée justifiant leur identité peuvent exiger du responsable d'un site internet qu'il « prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence ». Mais la loi ne prévoit aucune transmission des droits du défunt aux héritiers. L'héritier en question ne peut donc avoir accès aux données numériques du proche décédé.

Cependant, d'après la Cnil, les familles des personnes disparues qui s'adressent à elle « veulent pouvoir accéder aux données concernant le défunt ou exigent au contraire leur suppression ». La commission se trouve face à des problématiques techniques et juridiques : sans expression de la volonté du défunt, il est difficile d'agir.

La loi n'évoluant pas encore, faute de cas de jurisprudence, des start-up et les réseaux sociaux eux-mêmes commencent à proposer des fonctionnalités pour paramétrer sa mort numérique.

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

Source : http://www.ouest-france.fr/sur-les-reseaux-sociaux-il-y-aura-bientot-plus-de-morts-que-de-vivants-3194974
Par Jeanne HUTIN

Protection des données personnelles : le pas en arrière de l’Europe | Le Net Expert Informatique

Protection des données personnelles : le pas en arrière de l’Europe

L'avenir de la protection des données en Europe se décide au Conseil. Et cet avenir ne s'annonce pas radieux au vu des modifications proposées. Quatre associations de protection ont eu accès aux derniers brouillons et dénoncent un recul des droits.

Depuis 2012, la nouvelle réglementation relative à la protection des données personnelles est en discussion en Europe. Mais le texte a déjà pris au moins une année de retard, en raison notamment des blocages au sein du Conseil.
Et rien ne garantit que ce contretemps sera mis à contribution pour accroître la protection des individus. C'est le constat que dressent quatre associations de protection de la vie privée (Privacy International, EDRi, Access et Panoptykon Foundation) qui ont eu accès aux derniers brouillons du projet débattu au sein du Conseil de l'Europe.

Une réforme sapée par le Conseil
« Malheureusement, au sein du Conseil de l'UE, les gouvernements des Etats membres travaillent à saper ce processus de réforme. Durant plus de trois ans, le Conseil n'a pas seulement échoué à afficher un soutien à cette réforme et aux négociations, mais propose désormais des modifications du texte qui pourraient abaisser le niveau de protection actuel des données en Europe » dénoncent-elle dans un rapport.
Pour les organisations, la protection des données personnelles repose en grande partie sur le principe du consentement. Or, en se basant sur les propositions du Conseil, et en particulier de l'Allemagne, elles observent un profond recul par rapport à la proposition initiale en estimant que le paramétrage du navigateur vaudrait consentement de l'internaute en matière de suivi et de profilage.
L'Allemagne est accusée outre de défendre la possibilité pour les entreprises de procéder à une collecte et à un traitement de données sans recueil préalable du consentement dès lors que l'exploitation répond à un « intérêt légitime ».
« Ces données pourraient être transmises à des tiers sur la base de cette exception d'intérêt légitime et ces tiers pourraient utiliser cette exception pour commencer à traiter des données pour des finalités sans aucun lien ou incompatibles avec l'objectif initial » commente le rapport.
Sur la question de l'information, un recul des droits est également dénoncé. Le Conseil de l'UE propose ainsi de supprimer l'article 11 du texte. Or celui-ci définit concrètement les obligations relatives à l'information des individus, et notamment des enfants, sur la façon dont leurs données personnelles sont utilisées.

Les sanctions pourraient baisser
Les gouvernements préconisent également d'ajouter une exception permettant d'établir des profils des citoyens au nom de l'intérêt public, comme par exemple pour des raisons de sécurité nationale et de défense. Et la liste n'est pas exhaustive, laissant aux Etats la possibilité d'ajouter des exceptions.
Sur le front des sanctions et des actions en justice, les organisations de protection s'inquiètent là aussi d'une régression. Selon elles, les modifications introduites par le Conseil retirent la possibilité de mener des actions collectives. Des membres feraient également pression en faveur de sanctions plus légères, inférieures aux 5% de CA annuel prévus initialement.
Le guichet unique enfin. Censé apporté une simplification administrative, il serait au contraire en passe de se complexifier. Dans le cas de plaintes transnationales, au moins deux autorités de protection devraient être impliquées. Le Bureau européen de la protection des données interviendrait lui en cas de conflit dans la résolution d'un litige entre deux autorités ou plus.
Les désaccords autour du guichet unique ne sont pas nouveaux. Loin d'être une source de simplification, celui-ci constituerait avant tout un cadeau fait aux géants du Web, lui reprochent plusieurs autorités de protection. La présidente de la Cnil s'est d'ailleurs déclarée contre le principe de ce guichet tel qu'imaginé au départ.

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

Source :
http://www.zdnet.fr/actualites/protection-des-donnees-personnelles-le-pas-en-arriere-de-l-europe-39815834.htm

Écoute téléphonique des salariés : création de la norme simplifiée n°57 par la CNIL | Le Net Expert Informatique

Écoute téléphonique des salariés : création de la norme simplifiée n°57 par la CNIL

La CNIL, le 27 novembre 2014, a offert aux entreprises une nouvelle norme simplifiée pour leur permettre de déclarer rapidement et facilement les traitements de données relatifs à l'écoute et à l'enregistrement des conversations téléphoniques sur le lieu de travail. Il s'agit de la norme simplifiée n°57.

Puisque l'informatique est partie inhérente de l'entreprise il revient à l'employeur de prendre les mesures adéquates et légales pour mettre en œuvre ses traitements de données de salariés.

Or, tout traitement de données à caractère personnel doit faire l'objet d'une déclaration préalable à la CNIL. Il s'agit par exemple du traitement de gestion des badges d'accès aux locaux, de la messagerie électronique, le cas échéant, la vidéosurveillance ou encore tout traitement ayant pour finalité le contrôle de l'activité des salariés. C'est donc bien le cas pour l'écoute des salariés.

A cette fin, l'entreprise doit adhérer à la norme simplifiée n°57 pour tout traitement de données à caractère personnel destinés à l'écoute et l'enregistrement ponctuel des conversations téléphoniques sur le lieu de travail à des fins de formation et évaluation des employés ainsi que l'amélioration de la qualité du service fourni.

Attention il est impératif de respecter le contenu de la norme. A défaut la déclaration à la CNIL ne serait pas prise en compte. Il faut donc relire la norme simplifiée n°57 et mettre à jour ses processus internes afin de la respecter, par exemple pour les durées de conservation.

Cette déclaration à la CNIL n'est pas la seule formalité à respecter, en effet comme toute modification des conditions de travail, la mise en place d'un dispositif d'écoute des salariés doit être soumise à l'information et la consultation des instances représentatives du personnel.

La mise en place de telles écoutes permet à l'employeur de collecter notamment des données sur l'activité des salariés.

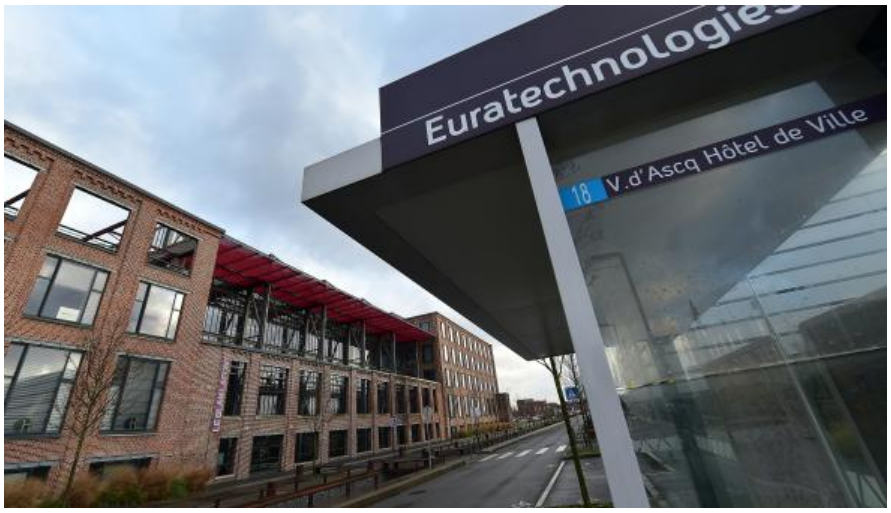
A défaut de déclaration à la CNIL, il y a un risque important pour l'employeur qui réside dans l'impossibilité d'utiliser les données collectées par l'entreprise dans le cadre d'une procédure de licenciement d'un salarié.

A NOTER : la jurisprudence de la Chambre sociale de la Cour de cassation du 8 octobre 2014 rappelle que la déclaration de ces dispositifs de collecte de données des salariés doit être préalable à leur mise en œuvre. A défaut, tout licenciement basé sur des preuves collectées par ce dispositif d'écoute serait jugé sans cause réelle et sérieuse pour illicéité de la preuve.

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

Source :
http://www.village-justice.com/articles/ecoute-telephonique-des-salaries,19088.html
Par Yaël Cohen-Hadria, Avocat

« On peut abattre une entreprise avec une attaque informatique » | Le Net Expert Informatique



« On peut abattre une entreprise avec une attaque informatique »

La sécurité informatique est aujourd'hui un enjeu majeur pour nos sociétés. Lors du dernier Forum international de la cybersécurité à Lille, le Clubster cybersécurité et confiance numérique a été lancé en Nord-Pas-de-Calais. La filière s'organise, tout comme nos entreprises.

Toutes les secondes, 49 % des internautes dans le monde sont victimes d'actes malveillants. En une semaine, une entreprise peut subir jusqu'à 1400 attaques informatiques de plus ou moins grande importance. Chaque année, la cybercriminalité coûte 2,5milliards d'euros à la France. Huit des dix objets connectés les plus populaires (ordinateur, smartphone, etc.) peuvent présenter un risque pour la vie privée. Plus de 90 % des 64000 cyberinfractions recensées en 2013 par l'Observatoire national de la délinquance et des réponses pénales (ONDRP) sont des escroqueries et des attaques financières.
On l'aura compris, protéger ses données et ses échanges informatiques est un enjeu majeur tant pour les entreprises que pour n'importe quel citoyen.
Lors du dernier Forum international de la Cybersécurité qui s'est tenu à Lille, la Région a lancé le Cluster Cybersécurité et confiance numérique, premier du genre en France. Une centaine d'entreprises, écoles et universités, laboratoires et institutions représentant 6500 salariés, décident de travailler ensemble pour faire décoller une vraie filière, générant déjà un chiffre d'affaires de près de 535millions d'euros.

Grands noms
« Nous avons là un secteur prometteur avec des croissances de marché énorme », constate Raouti Chehih, directeur d'Euratechnologies qui héberge le cluster. Au printemps, un incubateur va être lancé pour accueillir les jeunes pousses les plus prometteuses en matière de cybersécurité.
« Notre région a déjà une forte expérience avec ses grands noms de la distribution, de la finance, de la santé, qui génèrent de forts besoins en matière de sécurité informatique. » Les innovations émergent (lire ci-contre). Le lillois Dhimyotis est le leader français dans le domaine de la certification et de la signature électronique. Le seul éditeur français d'antivirus, AxBx, est à Villeneuve-d'Ascq. À nous de nous imposer parmi les meilleurs.

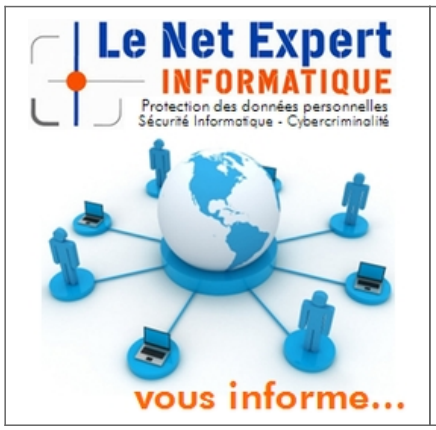
UNE SIMPLE ATTAQUE PEUT RUINER VOTRE BUSINESS
Il y a eu l'affaire Snowden, du nom de l'informaticien qui a révélé le programme de surveillance informatique de masse des services secrets américains. Il y a eu le blocage complet du site américain de Sony. Il y a eu le pillage de 40millions de données clients du géant de la distribution américaine Target…
« Dans une société totalement connectée, on voit une explosion des menaces sur les réseaux informatiques. On a de l'escroquerie, des attaques entre États, de l'espionnage industriel, du terrorisme. C'est sur tous ces fronts qu'il faut travailler. » Pierre Calais est le directeur général adjoint de Stormshield à Villeneuve-d'Ascq. La société, fruit du rapprochement entre la société nordiste Netasq et la société lyonnaise Arkoon, et filiale d'Airbus Defence and Space, est surtout le numéro un européen en matière de sécurité informatique (220salariés dont 80 à Villeneuve-d'Ascq).
« La maîtrise de la technologie est aussi une question de confiance et de souveraineté. Nous sommes aujourd'hui encore trop dépendants des technologies américaines et désormais chinoises. Il est fondamental de maîtriser la sécurité des systèmes d'information pour garder son indépendance. C'est aussi cela l'enjeu du cluster cybersécurité qui se développe dans notre région. »
Stormshield développe, pour les plus grands noms de l'industrie et de la défense, tout un panel de systèmes de protection et de sécurité des réseaux. « Un simple anti-virus ou pare-feu ne suffit plus. Il faut aussi protéger des menaces inconnues. Pour cela il faut détecter très vite les comportements anormaux sur les réseaux, les données, les postes de travail comme les réseaux, pour pouvoir les bloquer. »
Et l'enjeu ne concerne pas que les grandes entreprises. « Les PME et TPE croient souvent qu'elles ne manipulent pas de données importantes. Mais toutes les entreprises possèdent des fichiers clients et des données qui peuvent intéresser des pirates. Aujourd'hui, on peut mettre le business d'une entreprise par terre seulement avec une attaque informatique. Et les plus petites entreprises sont les plus vulnérables, car les moins protégées, par ignorance, ou par souci d'économie. »
C'est souvent après un cambriolage que l'on pense à mettre une alarme. Mais il est trop tard…
Lire la suite….

Expert Informatique 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 protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.lavoixdunord.fr/economie/cybersecurite-on-peut-abattre-une-entreprise-avec-ia0b0n2692787

Les entreprises qui appliquent des mesures de protection des données personnelles jouissent d’une meilleure réputation, les clients leur font davantage confiance et elles se démarquent clairement sur le marché



Les entreprises qui appliquent des mesures de protection des données personnelles jouissent d’une meilleure réputation, les clients leur font davantage confiance et elles se démarquent clairement sur le marché

L’absence d’accord au niveau européen conduit les entreprises à différer toute action au profit de celles qui appliquent des règles strictes de sécurité et de confidentialité déjà en place.

Le fait que les efforts d’harmonisation des règles européennes de collecte, d’utilisation et de conservation des données s’enlisent dans des débats politiques, pourrait bien faire perdre une part substantielle de leur avantage concurrentiel à la majeure partie des entreprises de l’UE qui avouent être mal préparées aux changements à venir[i], selon Iron Mountain, le spécialiste des services de conservation et de gestion de l’information.
Dans un document consultatif*, Iron Mountain souligne l’importance pour les entreprises de mettre en œuvre de solides mesures de protection des données, indépendamment de ce que préconisent les propositions réglementaires. En effet, il est démontré que **les entreprises qui appliquent de telles mesures jouissent d’une meilleure réputation, que les clients leur font davantage confiance et qu’elles se démarquent clairement sur le marché**.

Forrester avance que « dans la lutte pour acquérir, servir et fidéliser les clients, la sécurité des données et le respect de la confidentialité sont aujourd’hui des gages qui aident à se différencier de la concurrence ».[ii]

Ce document aide les entreprises à mesurer pleinement les effets de la nouvelle réglementation et à comprendre leur importance. Bon nombre de dispositions font toujours l’objet d’intenses débats parmi les dirigeants de l’UE trois ans après la première proposition de loi : celles relatives aux données du secteur public, le droit d’accès aux données par les organismes chargés de l’application de la loi et la possibilité pour les entreprises internationales de traiter directement avec le régulateur sur leur marché d’origine (le « guichet unique »), . Le retard pris pour parvenir à un accord ne reflète pas uniquement les intérêts divergents des 28 États membres, mais aussi l’évolution rapide des technologies, des nouveaux consommateurs connectés et du Big Data.
« La proposition de loi est extrêmement puissante et elle aura des répercussions dans le monde entier », déclare Edward Hladky, Directeur Général Adjoint d’Iron Mountain France. « Certains concepts seront étudiés de près dans quelques zones géopolitiques : la cohérence des règles et leur mise en œuvre à travers les frontières, le droit à l’oubli et le besoin d’une désidentification efficace des données personnelles utilisées dans les secteurs de la santé et de la recherche. »
« Toutefois, avec autant de propositions en constante évolution, les entreprises peuvent être tentées d’attendre de voir ce que la version finale contiendra réellement. Nous pensons que ce serait une erreur. L’éthique veut que les organisations protègent les données fermement et efficacement et qu’elles les utilisent et les conservent de manière responsable et transparente. Autant cela renforce la confiance des clients, autant les violations de données les rendent méfiants. L’équation est simple : la confiance nourrit la fidélité et la fidélité nourrit les ventes. Les entreprises ont beaucoup à gagner en agissant dès maintenant, avant que la loi les oblige à le faire. »

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

Source : http://www.infodsi.com/articles/154353/attente-nouvelle-legislation-europeenne-protection-donnees-pourrait-couter-cher-competitivite-image-marque-entreprises.html
* Le livre blanc, en version anglaise, édité pour la journée européenne de la protection des donnes, « An opportunity to plan and manage the impact of legal change » est disponible sur http://www.ironmountain.co.uk/services/dpd.aspx

[i]52 % des entreprises d’après une étude menée au Royaume-Uni, en Allemagne et en France par Ipswitch Software en octobre 2014. http://www.techweekeurope.co.uk/e-regulation/european-teams-woefully-unprepared-general-data-protection-regulation-155316#ArDP0sA9ymVzYTPT.99
[ii]https://www.forrester.com/Predictions+2015+Data+Security+And+Privacy+Are+Competitive+Differentiators/fulltext/-/E-RES116328