Données personnelles : mais à quoi sert la CNIL ? – Cash Investigation ce mardi 6 octobre 2015 | Le Net Expert Informatique

Données personnelles : mais à quoi sert la CNIL ? – mardi 6 octobre 2015

Certaines associations caritatives vendent en toute illégalité leurs fichiers de donateurs à La Poste. Face à Elise Lucet, la présidente de la CNIL ne semble pas au courant et se déclare « surprise ». Un extrait de « Cash Investigation » diffusé sur France 2 le mardi 6 octobre à 20h55. Lire la suite….
Ci-dessous, le rapport d'activité 2014 de la CNIL dont il est fait mention dans le reportage (Merci à Eric EGÉA) :
http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-35e_rapport_annuel_2014.pdf.pdf

---

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. 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

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

Source : http://www.francetvinfo.fr/internet/cash-investigation-donnees-personnelles-mais-a-quoi-sert-la-cnil_1109973.html

Windows 10 et sa vie privée, la CNIL met en garde et propose une fiche pratique | Le Net Expert Informatique

	Windows 10 et sa vie privée, la CNIL met en garde et propose une fiche pratique

Windows 10 est disponible gratuitement pour les PC sous Windows 7 ou Windows 8.1. Il propose des changements face à ses prédécesseurs dont certains touchent à la surveillance, l'analyse et la collecte de données personnelles concernant ses utilisateurs. La CNIL met en garde et propose un tutoriel pour se protéger des yeux indiscrets de la firme.

En France, la CNIL a rapidement réagi devant les nombreux systèmes de surveillance et de collecte de données accompagnant Windows 10. Dans un dossier mis en ligne quelques jours seulement après le lancement de l'OS, elle propose « quelques réglages de confidentialité qui permettent de limiter la communication de vos informations à l'éditeur et à ses partenaires ».

Windows 10, des fuites dans Cortana, Microsoft Edge ou encore la synchronisation

Ils se concentrent sur trois thèmes, Cortana avec un paramétrage de la » vie privée « , la synchronisation des comptes sur les autres appareils utilisés et le navigateur Microsoft Edge.

Elle recommande ainsi de désactiver la géo-localisation, d'empêcher la collectes de données liées à l'Appareil photo, le Microphone, les Informations de Compte, des Contacts, du Calendrier, de la Messagerie, des communications Radio ou encore d'agir sur la fonctionnalité » apprendre à me connaître » pour la dictée vocale. Au sujet du nouveau navigateur, Microsoft Edge, il est recommandé de désactiver l'option » Utiliser la prédiction de page pour accélérer la navigation, et améliorer le mode lecture ainsi que mon expérience globale » puisque celle-ci requiert d'envoyer votre historique de navigation tandis l'obtention de suggestions de recherche demande qu'une grande partie des informations que vous saisissez dans la barre de navigation soit envoyée au moteur de recherche Bing. Il est donc recommandé de désactiver « Afficher les suggestions de recherche à mesure que je tape « .

Vous trouverez ici, un pas à pas complet pour reprendre la main sur vos données personnelles : Régler les paramètres vie privée de Windows 10

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

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

Source :
http://www.ginjfo.com/actualites/logiciels/windows-10/windows-10-et-sa-vie-privee-la-cnil-met-en-garde-et-une-fiche-pratique-20150928

Safe Harbor remis en question – Et si le transfert de

données personnelles aux US cessait ? | Le Net Expert Informatique

Safe Harbor remis en question – Et si le trans

Pour l'avocat général de la CUJE, la disposition autorisant les transferts de données vers les Etats-Unis (Safe Harbor) est invalide car le pays ne garantit pas la protection de ces données du fait de la surveillance par la NSA. Une Cnil européenne a de plus tout pouvoir pour suspendre ces transferts.

Entre Maximilian Schrems et Facebook, c'est une longue histoire d'amour (vache). C'est notamment à ce dernier qu'on doit d'avoir découvert l'ampleur de la collecte de données personnelles effectuée par le réseau social.
Remonté contre les pratiques de Facebook, le jeune autrichien l'est tout autant à l'encontre de la surveillance massive par les Etats-Unis. Pour accéder aux données des Européens, la NSA pourrait compter sur un dispositif : le Safe Harbor.

Une « des voies » des agences US pour accéder « à la collecte des données »

Le Safe Harbor prévoit le transfert automatique de données par les entreprises entre l'Europe et les Etats-Unis. C'est cet accord qui est visé par Maximilian Schrems au travers de sa plainte contre Facebook devant la justice irlandaise.
Le justiciable européen conteste le transfert de données à caractère personnel de Facebook Ireland à Facebook USA au motif que la protection de ses données n'est pas garantie du fait du programme PRISM de la NSA.
Saisie par la Haute Cour de Justice d'Irlande, la Cour de Justice européenne est appelée à se prononcer sur plusieurs points de droit. Pour l'heure, c'est l'avocat général de la CUJE, Yves Bot, qui a livré son analyse juridique.

Et en substance, ce dernier souligne le manque de garanties entourant le Safe Harbor et estime qu'une autorité nationale de protection peut enquêter sur les transferts de données réalisées dans ce cadre.

Plus encore, écrit l'avocat général, une autorité, au terme de ses investigations, « a le pouvoir de suspendre le transfert de données en cause » dès lors qu'elle estime qu'il « porte atteinte à la protection dont doivent bénéficier » les citoyens de l'UE.
Le Safe Harbor part du postulat que les Etats-Unis apportent un niveau de protection adéquat. Une obligation cependant qui se doit d'être continue, souligne Yves Bot. Cela « suppose qu'aucune circonstance intervenue depuis ne soit de nature à remettre en cause l'évaluation initiale effectuée par la Commission. »
Or, les révélations d'Edward Snowden au sujet de la surveillance par la NSA pourraient justement constituer une remise en cause. La Commission de l'UE elle-même estimait que le Safe Harbor était « l'une des voies par lesquelles les autorités américaines de renseignement ont accès à la collecte des données à caractère personnel initialement traitées au sein de l'Union. »

La « décision 2000/520 doit être déclarée invalide »

Pour l'avocat général de la CUJE, le « droit et la pratique des États-Unis permettent de collecter, à large échelle, les données à caractère personnel de citoyens de l'Union qui sont transférées dans le cadre du régime de la sphère de sécurité, sans que ces derniers bénéficient d'une protection juridictionnelle effective. »
C'est donc le principe même du Safe Harbor et des transferts automatisés de données qui est contesté. « Nous sommes, dès lors, d'avis que la décision 2000/520 doit être déclarée invalide dans la mesure où l'existence d'une dérogation qui permet d'une manière aussi générale et imprécise d'écarter les principes du régime de la sphère de sécurité empêche par elle-même de considérer que ce régime assure un niveau de protection adéquat aux données à caractère personnel qui sont transférées aux États-Unis depuis l'Union » va jusqu'à considérer le représentant de la CUJE.
« C'est formidable de voir que l'avocat général a utilisé cette affaire pour rendre un avis général sur les transferts de données vers des pays tiers et la surveillance de masse » réagit Maximilian Schrems.
« Si le système du Safe Harbor disparaît, il est très probable que les autorités de protection dans les 28 Etats membres de l'UE n'autoriseront pas les transferts de données des entreprises US soumises à des lois de surveillance de masse » ajoute-t-il.
Les géants américains du Web comme Facebook pourraient ainsi se voir interdire le droit de transférer les données des utilisateurs européens de leurs services vers les Etats-Unis. Les juges de la Cour de Justice de l'UE doivent toutefois rendre leur décision, en tenant compte ou non de l'avis de l'avocat général.

Source : http://www.zdnet.fr/actualites/safe-harbor-et-si-le-transfert-de-donnees-personnelles-aux-us-cessait-39825358.htm
Par Christophe Auffray

L’Europe pourrait revoir le transfert de données personnelles vers les Etats-Unis | Le Net Expert Informatique

L’Europe pourrait revoir le transfert de données personnelles vers les Etats-Unis

La justice européenne met un coup de canif dans le processus permettant aux services américains de puiser dans les informations personnelles d’internautes européens. Suite à une plainte concernant Facebook, l’avocat général de la CJUE demande qu’un pays puisse en demander l’arrêt.

Le Safe Harbor est un texte datant de 2000 autorisant, sous certaines conditions, des entreprises américaines à transférer des données personnelles présentes en Europe vers leur territoire. Un principe qui soulève des polémiques depuis les révélations autour de systèmes américains (NSA via le dispositif PRISM) permettant de consulter ces informations.
La justice européenne souhaite à présent revoir ce dispositif. L’avocat général de la Cour de Justice de l’Union européenne (CJUE) vient à ce titre de rendre un avis dans lequel il demande à ce que n’importe quel Etat membre puisse mettre en pause ce transfert de données. En conséquence, les services américains du renseignement ne pourraient plus puiser dans ce vaste vivier d’informations.
S’il ne s’agit ici que d’un avis (http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106fr.pdf) émis par l’avocat général Yve Bot sur l’épineuse question de la protection des données personnelles, le document demeure clair à l’encontre de la pratique. Il motive son avis en évoquant les cas de « défaillances systémiques constatées dans le pays tiers vers lequel des données à caractère personnel sont transférées, les États membres doivent pouvoir prendre les mesures nécessaires à la sauvegarde des droits fondamentaux protégés par la Charte des droits fondamentaux de l’Union européenne, parmi lesquels figurent le droit au respect de la vie privée et familiale et le droit à la protection des données à caractère personnel ».
Autrement dit, la justice considère que ce principe de transfert automatique de données constitue une « ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données ». Elle demande donc à ce que les autorités nationales de protection des informations personnelles puissent conserver la main sur ce type d’activité.

Max Schrems, un étudiant autrichien au début de la polémique

Depuis à présent 4 ans, Max Schrems, un jeune autrichien s’attaque aux pratiques de Facebook en matière de conservation et de protection des données de ses utilisateurs. Après avoir en premier lieu reproché au réseau social de créer des profils fantômes de personnes inexistantes, il avait attaqué le service pour avoir communiqué à la NSA des informations sur ses inscrits, notamment dans le cadre du programme PRISM.
L’affaire avait été portée devant la Data Protection Commissioner (DPC), l’équivalent de la Cnil en Irlande puis auprès de la Haute Cour du pays (Etat dans lequel le siège de Facebook Europe se trouve). Le cas est ensuite remonté jusqu’à la CJUE.
Suite à la remise de cet avis, la question de la suspension du Safe Harbor se pose à nouveau. La Cour de justice peut désormais suivre ou non l’avis de l’avocat général avant de remettre sa décision définitive. Celle-ci devrait survenir dans les prochains mois.

Source :
http://pro.clubic.com/blog-forum-reseaux-sociaux/facebook/actualite-780512-facebook-europe-cour-justice.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1165961926#pid=22889469

Nouveau règlement européen sur la protection des données personnelles : Les changements pour les entreprises | Le Net Expert Informatique

Nouveau règlement européen sur la protection des données personnelles : Les changements pour les entreprises

Fin juillet, le Contrôleur Européen de la Protection des Données a publié ses recommandations sur le futur règlement européen portant à quatre le nombre de versions du document. L'occasion de faire le bilan sur les trois évolutions du règlement qui auront le plus d'impact pour les entreprises.

QUEL CHANGEMENT POUR LES ENTREPRISES ?

Mise en place du Privacy by Design (Articles 23, 30, 32a, 33a et 33)

Première nouveauté, les entreprises devront définir et mettre en œuvre des procédures permettant d'intégrer les problématiques liées à la manipulation des données personnelles dès la conception de nouveaux services.

Cette démarche s'accompagne de l'obligation de réaliser des analyses de risques relatives à la vie privée des personnes (discrimination, diffusion de données confidentielles, etc.) préalablement à la mise en place des traitements les plus sensibles et à chaque modification du traitement.

Face aux risques sur la vie privée des personnes induits par ces traitements, il sera imposé aux entreprises d'adopter des mesures de sécurité adéquates en vue de les maitriser.

Concrètement que retenir du Privacy by Design ?

Une mise à jour de la méthodologie projet afin d'identifier au plus tôt les traitements sensibles et une méthode d'analyse de risques à définir et outiller.

Il sera pour cela possible de s'inspirer des guides pratiques de la CNIL intitulés « Etude d'impact sur la vie privée », qui seront à simplifier et contextualiser aux besoins spécifiques de l'entreprise.

Responsabilisation ou « Accountability » (Articles 22 et 28)

Toute entreprise devra désormais être capable de prouver sa conformité vis-à-vis du règlement.

Cette exigence se traduit par :

• l'adoption d'une politique cadre de gestion des données à caractère personnel ;

• une organisation associée ;

• des procédures opérationnelles déclinant les thèmes du règlement (information, respect des droits des personnes, transfert à des sous-contractants, etc.).

L'entreprise devra également être en capacité de prouver l'application de ces politiques et donc, de mettre en place des processus de contrôle.

L'occasion de parler de la personne qui illustrera ce principe d' « Accountability » : le DPO (pour Data Protection Officer). Il devient quasiment obligatoire et remplace le CIL actuel.

Concernant ce DPO, le texte entérine l'obligation de lui fournir le personnel, les locaux, les équipements et toutes les autres ressources nécessaires pour mener à bien ses missions. Encore une fois le parlement souhaite aller au-delà de cette exigence : il propose de nommer au sein de la direction une personne responsable du respect du règlement.

Comment appliquer ce principe ? Il sera nécessaire de définir a minima une politique avec des règles de protection des données ainsi qu''un plan de contrôle et de formation. Cette politique pourra par exemple s'inspirer du modèle des BCR « Binding Corporate Rules », dont le principe a été entériné dans le futur texte, pour lesquelles des modèles types et des premiers retours d'expérience existent déjà.

Obligation de notification des fuites (articles 31 et 32)

L'ensemble des parties s'accordent sur l'obligation de notification des fuites aux autorités. Le Parlement propose même que les entreprises mettent en ligne un registre listant les types de brèches de sécurité rencontrées. Il sera intéressant de constater comment cette exigence cohabitera avec les législations nationales en matière de sécurité et la protection des intérêts de la nation qui tendent à limiter la diffusion de ce type d'information.

La notification de fuites aux personnes concernées, quant à elle, n'est obligatoire que si l'entreprise n'est pas en mesure de démontrer qu'elle a mis en œuvre des mesures afin de rendre cette fuite sans conséquence. D'où l'intérêt d'effectuer correctement l'analyse de risques, de définir et d'implémenter des mesures appropriées.

Au final, deux recommandations afin d'anticiper le futur règlement sur ce point :

• un processus de gestion des fuites de données à définir en l'orchestrant avec les dispositifs de gestion de crise existants et les processus de relation client,

• la réalisation d'exercices réguliers afin de tester son efficacité avec tous les acteurs concernés.

UNE MISE EN CONFORMITÉ À ANTICIPER

Au-delà de ces trois nouveautés majeures, d'autres modifications plus limitées en termes d'impacts organisationnels sont également à prendre en compte, comme la création du droit à la portabilité ou l'extension de la liste des données sensibles. On peut par ailleurs noter le renforcement d'obligations existantes comme le droit à l'information et le recueil du consentement. Le diable se nichera dans les détails.

Pour conclure, les deux années de mise en application du règlement ne seront pas de trop (soit une mise en conformité d'ici début 2018) et nous ne pouvons que conseiller d'initier la mise en conformité dès 2016, avec le cadrage et le lancement des premiers chantiers majeurs. D'autant plus que le sujet devient de plus en plus visible médiatiquement (condamnation récente de Boulanger, Google et l'application du droit à l'oubli, etc.) et que les sanctions financières deviennent réellement significatives (entre 2 et 5% du chiffre d'affaire mondial). L'occasion pour toutes les entreprises de communiquer largement sur les principes de respect de la vie privée effectivement appliqués.

Source : http://www.solucominsight.fr/2015/09/nouveau-reglement-europeen-sur-la-protection-des-donnees-personnelles-anticiper-les-3-impacts-majeurs/

Géolocalisation des véhicules professionnels des employés : que faire si mon employeur ne respecte pas les règles ? | Le Net Expert Informatique

Géolocalisation des véhicules professionnels des employés : que faire si mon employeur ne respecte pas les règles ?

Vous avez plusieurs recours :
• Adresser une plainte à la CNIL : la CNIL peut contrôler tous les systèmes de géolocalisation installés en France. Si le contrôle confirme que l'employeur ne respecte pas les règles, il sera mis en demeure de respecter la loi, sous peine de sanctions ;
• Saisir les services de l'inspection du Travail de votre département ;
• Déposer une plainte pénale auprès du procureur de la République, des services de police ou de gendarmerie.
• Vous avez demandé à avoir accès aux informations de géolocalisation qui vous concernent et votre employeur a refusé ?

Vous pouvez, après un délai de 2 mois, adresser une plainte à la CNIL.

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. 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

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

S o u r c e :
https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=06EF1A234FB5C655BF980F0F5D5C31E9?name=G%C3%A9olocalisation+des+v%C3%A9hicules+professionnels+des+employ%C3%A9s+%3A+que+faire+si+mon+employeur+ne+respecte+pas+les+r%C3%A8gles+%3F&id=339

Un électeur peut-il utiliser

la liste électorale ? | Le Net Expert Informatique

Un électeur peut-il utiliser la liste électorale ?

Tout électeur peut obtenir de sa mairie une copie de la liste électorale à condition de s'engager à ne pas en faire un usage commercial.
A noter : la Commission d'accès aux documents administratifs (CADA) considère que l'accès aux listes électorales peut s'exercer par consultation gratuite sur place ou par envoi de copies, sur support papier ou informatique.

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

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

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

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=16F67A95B36120F226D2F8E337B98601?name=Liste+%C3%A9lectorale+%3A+un+%C3%A9lecteur+peut-il+l%27utiliser+%3F&id=175

L'Europe prend un mauvais virage en matière numérique | Le Net Expert Informatique

L’Europe prend un mauvais virage en matière numérique

Dans l'exercice consistant à élaborer de bonnes politiques en matière numérique, l'Europe a raté son premier test majeur. Au mois de mai, la Commission européenne annonçait la création d'un marché unique du numérique réunissant 500 millions de consommateurs, censé apporter 415 milliards € au PIB de l'Union européenne et créer quelque 3,8 millions d'emplois. Seulement voilà, une récente décision autour d'une problématique numérique majeure – la confidentialité des données – menace de faire dérailler la locomotive.

Au mois de juin, les ministres de l'Intérieur et de la Justice de l'UE ont voté en faveur de la conservation de pouvoirs nationaux significatifs en matière de protection de la confidentialité numérique, plutôt que d'élaborer un ensemble de règles s'appliquant aux 28 Etats de l'UE. Si le Parlement européen venait à approuver cette proposition, la divergence des règles nationales serait alors de retour. Plus inquiétant encore, ceci ouvrirait la voie à la mise en place de dispositions rendant illégales les activités bénignes et peu risquées d'exploration des données, qui sous-tendent la publicité en ligne.

La publicité sur Internet permet aux citoyens de l'UE d'accéder à de l'information, à des contenus éducatifs, à des canaux de commerce et autres sites de divertissement, sans avoir à en payer directement l'accès. En Europe, les montants dépensés dans ce domaine sont en pleine augmentation. Les revenus du secteur ont plus que quadruplé depuis 2006, malgré la stagnation de l'économie européenne dans son ensemble. Le nouveau combat de la confidentialité en UE vient menacer toute cette évolution. Non seulement faut-il s'attendre à une importante charge administrative liée aux coûts supplémentaires et aux difficultés bureaucratiques, mais un risque réel existe également de voir ces nouvelles règles mettre à mal le modèle d'entreprise d'un grand nombre des principales sociétés européennes en ligne.

Il s'agirait d'un véritable gâchis – qui plus est facilement préventible. En 2012, la Commission européenne a formulé une proposition de remplacement de la législation de l'UE existante en matière de protection des données, dont la plus récente version avait été élaborée en 1995, époque à laquelle Internet ne jouait qu'un rôle minime dans l'économie. Le texte initial était prometteur. Il entendait harmoniser les cadres juridiques fragmentés de l'Europe, fournir aux entreprises un guichet unique fort utile, et rassurer les consommateurs en leur garantissant une utilisation appropriée de leurs données.

Malheureusement, beaucoup des propositions les plus judicieuses ont été depuis abandonnées. Lors du rassemblement ministériel du mois de juin, le principe majeur de guichet unique a été véritablement éviscéré. Plutôt que de permettre aux entreprises d'avoir affaire à l'autorité de protection des données compétente au sein du pays dans lequel ces entreprises possèdent leur siège ou leur principale implantation européenne, les Etats membres insistent aujourd'hui pour que les régulateurs nationaux conservent le contrôle. Conformément aux nouvelles règles proposées, toute autorité « concernée » pourrait s'opposer à une décision prise par un autre régulateur national, donnant lieu à une procédure d'arbitrage complexe faisant intervenir l'ensemble des 28 agences.

Les ministres ont également adopté une large définition de ce que l'on entend par données personnelles. Y figureraient ainsi à la fois les cookies (petits ensembles de données stockés sur l'ordinateur d'un internaute) et les adresses IP (code utilisé pour identifier un ordinateur lorsqu'il se connecte à Internet) – bien que ces éléments ne fournissent aucun lien en direction d'un individu donné. Au mieux, cette définition étendue et peu pointue des données personnelles menace de créer des obstacles inutiles pour les annonceurs numériques basés dans l'UE. Au pire, elle risque de plonger leur modèle d'entreprise dans l'illégalité.

Ces règles inutilement strictes en matière de données sont vouées à affecter les entreprises européennes dans une mesure disproportionnée. On peut comprendre qu'il soit demandé à Google, Facebook et autres géants américains d'Internet de solliciter le consentement explicite de leurs utilisateurs. Pour autant, le secteur européen de l'Internet est dominé par des entreprises de B to B, dont les marques peu connues traitent effectivement les données des consommateurs, mais manquent d'un contact direct avec les utilisateurs. Ainsi, la seule véritable alternative consistera pour ces sociétés Internet européennes à travailler auprès des grandes plateformes américaines, et à devenir encore plus dépendantes de celles-ci.

Bien que le Royaume-Uni, la Suède, la Norvège et les Pays-Bas comptent parmi les pays leaders de l'Internet à travers le monde, de nombreux autres Etats européens évoluent considérablement à la traîne. Ainsi, l'économie numérique contribue au PIB de l'UE à hauteur d'environ 4 %, contre 5 % aux États-Unis et 7,3 % en Corée du Sud. Les nouvelles réglementations proposées ne feront qu'accentuer cet important retard des entreprises européennes par rapport à leurs concurrentes internationales.

L'Europe est confrontée à un choix important. Bien entendu, l'UE doit pouvoir rassurer ses citoyens quant à l'utilisation appropriée de leurs données ; les mesures en ce sens peuvent contribuer à la croissance de l'économie numérique. En revanche, les dirigeants du continent ne doivent pas oublier qu'un marché unique du numérique ne pourra exister aussi longtemps que les règles accentueront la divergence des approches nationales autour de la confidentialité, et qu'elles feront obstacle à l'utilisation par Internet des données anonymes à des fins de publicité numérique. Le sort d'une génération toute entière d'entrepreneurs numériques européens est aujourd'hui en jeu.

Source : http://www.libe.ma/L-Europe-prend-un-mauvais-virage-en-matiere-numerique_a66663.html

Par Christopher Engman PDG de la société suédoise de commercialisation en ligne, «Vendemore» (Traduit de l'anglais par Martin Morel)

Protection des enfants sur Internet : Leur vie privée pas respectée d'après la CNIL | Le Net Expert Informatique

Protection des enfants sur Internet : Leur vie privée pas respectée d'après la CNIL

29 autorités dans le monde ont mené un audit pour vérifier le respect des règles de protection de la vie privée par les sites internet consultés par les enfants. Cette opération montre que leurs données personnelles sont insuffisamment protégées

Les vérifications effectuées ont porté principalement sur : le type de données collectées, le niveau d'information et l'adaptation de l'information aux utilisateurs, la présence de mesures de vigilance ou de contrôle liées au jeune âge du public visé (quelles précautions particulières sont prises ?).

Ces vérifications font apparaître : une large collecte de données personnelles et peu de marge de manœuvre sur la suppression de comptes : 87 % (67% en moyenne pour les homologues) des sites examinés par la CNIL collectent des données personnelles (adresse IP, identifiant du terminal mobile, localisation), notamment à partir de la création obligatoire d'un compte utilisateur (nom, prénom, email). Si pour certaines de ces données, la collecte est justifiée par le service proposé par le site, pour d'autres, cette collecte n'est pas nécessaire. Seuls 39% de ces sites offrent à leurs utilisateurs une manière simple de supprimer leur compte ; un défaut de sensibilisation spécifique auprès des jeunes sur la collecte de leurs données : 71% des sites examinés comportent une mention d'information relative à la collecte de données à caractère personnel et notamment aux droits « informatique et libertés » des utilisateurs, mais seulement 33% adaptent l'information au jeune public visé et l'indiquent sur le formulaire rempli par l'enfant (ou son parent) ; une redirection courante vers des sites tiers, dont des sites marchands : sur 63 % des sites, les enfants peuvent être redirigés vers un autre site, y compris de type marchand, par un simple clic ; le dépôt de cookies sans bandeau d'information, une pratique encore très courante : tous les sites examinés déposent des cookies sur le terminal de l'utilisateur dès son arrivée sur la page d'accueil sans recueillir son consentement préalable et la plupart (63 %) sans l'apposition du bandeau d'information obligatoire

Les vérifications effectuées montrent également que trop de sites n'ont aucune mesure de vigilance : 62% de ces sites ne proposent aucune mesure de vigilance ou de contrôle parental à destination du jeune public (comme un message de sensibilisation ou l'envoi d'un email aux parents pour les informer de la collecte des données de leur enfant et leur demander leur accord).

Elle révèle enfin que la case de recueil de l'accord parental est la mesure la plus courante, mais est loin d'être généralisée : 18% des sites observés recueillent l'accord parental au moyen d'une case, 15 % introduisent une mesure de vérification de l'âge, 13 % incitent à la vigilance, 11% mettent en place un tableau de contrôle parental lors de la création du compte.

Au vu de ce constat, la CNIL donne des conseils à destination des gestionnaires de sites pour enfants et des parents.

Ainsi, elle publie deux fiches pratiques :pour accompagner les éditeurs dans la mise en conformité de leur site, avec conseils et mentions-types ; pour aider les parents à accompagner leurs enfants pour une navigation respectueuse de leur vie privée.

Les mesures prises par la CNIL à l'issue de cette campagne sont l'envoi d'un courrier aux éditeurs des sites pour enfants leur rappelant leurs obligations et les droits de leurs jeunes utilisateurs ; faute d'une mise en conformité de leur part, elle se réserve la possibilité d'effectuer de nouvelles vérifications et, le cas échéant, d'engager des procédures de sanction ; l'envoi d'un courrier aux associations de parents afin de les alerter sur les constats du « Sweep day » et construire avec eux une démarche de vigilance.

Source :
http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/126799/Vie-privee-des-enfants-une-protection-insuffisante-sur-les-sites-internet.aspx
http://www.cnil.fr/linstitution/actualite/article/article/vie-privee-des-enfants-une-protection-insuffisante-sur-les-sites-internet/
Par Lionel Costes

Droit à l'oubli : mode d'emploi pour demander la suppression de contenu ou photo | Le Net Expert Informatique

Droit à l'oubli : mode d'emploi pour demander la suppression de contenu ou photo

Comment demander la suppression d'un résultat de recherche Google, concernant une personne physique, qui enfreint le droit au respect de la vie privée.

Vous êtes victime d'une atteinte à votre réputation sur internet, d'une atteinte à votre image (par la publication de photos compromettantes ou tendancieuses), ou vous vous voulez faire supprimer des informations personnelles vous concernant des résultats de recherche de Google (par exemple le fait que vous avez eu une grave maladie, tel qu'un cancer, afin d'obtenir plus facilement une assurance de prêt immobilier). Voici la démarche à suivre.

Conformément à la décision de la Cour de justice de l'Union européenne du 13 mai 2014 (n°C-131/1), l'internaute français peut désormais signaler au moteur de recherche Google – qui concentre à lui seul 90% des requêtes faites sur le web – une demande de suppression d'un résultat de recherche qui contient à son égard des propos diffamations, inexacts, mensongers ou encore des informations confidentielles et personnelles sans son accord. C'est une obligation fondée sur le droit au respect de la vie privée, y compris lorsque cela concerne un compte Facebook.

En Europe, pour exercer le droit à l'oubli, il convient de s'adresser directement à Google, mais la CNIL peut aussi intervenir après un dépôt de plainte.

Toutefois, en juillet 2015, Google a fait savoir qu'il refusait d'étendre le droit à l'oubli aux noms de domaine dont l'extension est en « .com », c'est-à-dire la grande majorité des sites internet, déplore la CNIL ! Sur le blog européen du groupe, le responsable des questions de vie privée chez Google explique que le droit à l'oubli n'a pas à être appliqué à l'échelle globale, privant ainsi des centaines d'internautes français de leur droit.

Lire la suite….

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source :

http://www.net-iris.fr/veille-juridique/actualite/33376/droit-a-oubli-mode-emploi-pour-demander-la-suppression-de-contenu-ou-photo.php

Par Carole Girard-Oppici,