Une manière de nous espionner sur Internet sans laisser de traces !

Depuis plusieurs années, le mécanisme de suivi des internautes qui récupère votre « empreinte numérique » est utilisé par la société AddThis. Il serait installé sur plus de 5000 sites Web parmi les plus consultés, et surtout difficilement contournable.

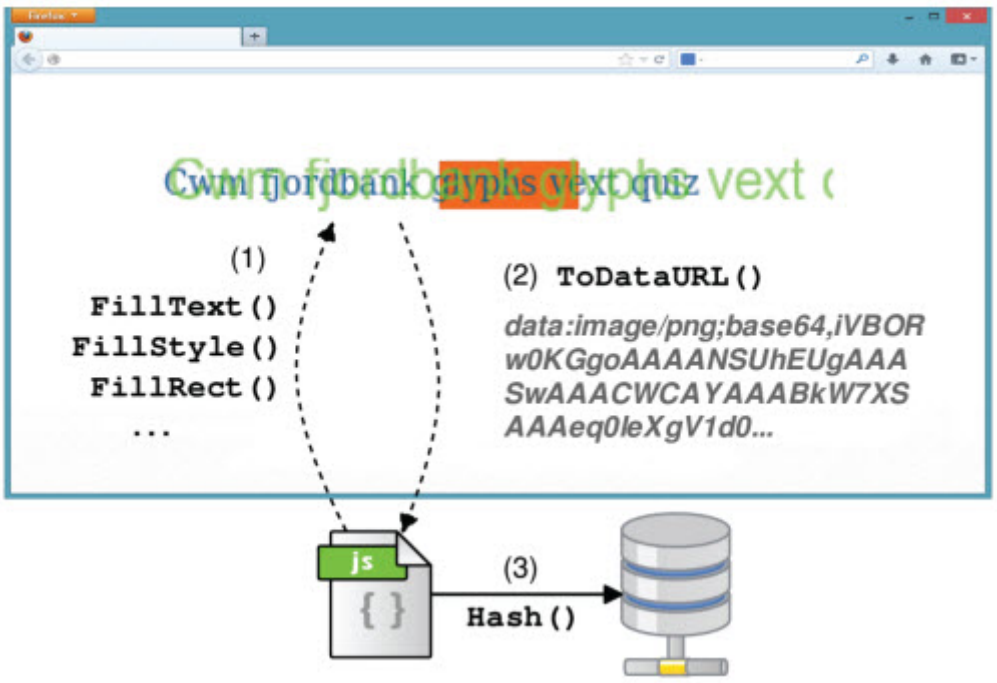
Atlantico, MetroNews, Letudiant, PAP, Telerama, Sports, Elle, LeGorafi… Ce sont autant de sites qui utilisent le fameux mécanisme d'empreinte numérique (la liste entière est consultable ici). Ce ne sont que quelques exemples français. Aux Etats-Unis, le site de la Maison-Blanche l'utilise également. S'il n'est pas tout à fait nouveau, il a été découvert assez récemment par des chercheurs des universités de Ku Leuven en Belgique, et de Princeton outre-Atlantique.

La nouveauté : il permet de traquer les internautes sans qu'ils s'en rendent compte et sans pouvoir y échapper. Car aucun mécanisme, une application tierce par exemple, ne permet de la contourner : le Graal pour les annonceurs, un fléau pour la vie privée ! Il existe toutefois des moyens d'y échapper,

en bloquant le chargement des JavaScript sur votre navigateur, en utilisant NoScript par exemple, en choisissant Tor ou l'extension (expérimentale) Chameleon.

Le mécanisme de fonctionnement de l'empreinte numérique.
Cette technique d'empreinte numérique, décrite par des chercheurs californiens en 2012 (consultez le PDF du détail de la technique), est notamment proposée dans les outils de la société AddThis, qui fournit entre autres des boutons de partage vers les réseaux sociaux.

Le système est très simple en théorie. Lorsqu'un internaute se connecte sur un site Web, une requête est envoyée demandant au navigateur de « dessiner » une image invisible qui est ensuite transmise à AddThis par exemple. Il utilise la fonction Canvas de HTML5 (« canvas fingerprinting »). Et c'est grâce à cette image unique qu'il est possible de pister discrètement et individuellement chaque internaute.



Dans cet article, on peut y voir AddThis reconnaître avoir commencé à tester ce système depuis le début de l'année cherchant « une alternative aux cookies traditionnels ». Depuis la publication de l'article, certains sites ont fait marche arrière, à l'instar de YouPorn notamment.

Le PDG de l'entreprise estime que le mécanisme est tout à fait légal, même si les premiers résultats ne seraient pas satisfaisants, selon lui. AddThis se défend sur son blog, expliquant que le mécanisme est utilisé uniquement dans un but de R&D. Il nous tarde de connaître la réaction de la CNIL : un mécanisme divulgué à tous et incontournable semble difficile à imposer en toute légalité…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.linformaticien.com/actualites/id/33713/tous-traques-addthis-nous-suit-a-la-trace-sans-laisser-de-traces.aspx

---

Les entreprises sous-estiment le risque juridique du Big

Data

Les entreprises sous-estiment le risque juridique du Big Data

Pour le Boston Consulting Group (BCG) et le cabinet d'avocats DLA Piper dans leur étude sur « Le Big Data face au défi de la confiance » publiée le 18 juillet 2014, l'exploitation de très nombreuses données peut exposer l'entreprise à des risques juridiques et économiques méconnus.

De fait, ils constatent que la surveillance exercée à grande échelle par la NSA sur les communications électroniques et téléphoniques, la navigation sur Internet et les réseaux privés ou encore les services de Cloud américains et étrangers, a heurté un public déjà très sensibilisé aux problématiques de protection des données. Ils rappellent que « certains acteurs clés d'Internet comme Google et Facebook ont été violemment critiqués après avoir modifié leurs règles de confidentialité ».

De plus, ils relèvent que la nouvelle réglementation européenne en cours d'élaboration aura « des incidences certaines sur les entreprises utilisant le Big Data (…). Le poids et le coût administratif du traitement de données pourraient augmenter. Cet ensemble de règles nouvelles pourrait aussi constituer une menace pour les stratégies de

monétisation de données, diminuer l'innovation et réduire les opportunités futures ».

« Le Big Data face au défi de la confiance », 18 juill. 2014 ; Site de BCG

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/124969/Default.aspx

---

La CNIL autorise la collecte de prévention de la délinquance pour les Collectivités locales

La CNIL autorise la collecte de prévention de la délinquance pour les Collectivités locales

La CNIL a adopté une nouvelle autorisation unique n° AU-038 par une délibération du 26 juin 2014 « portant autorisation unique concernant les traitements de données relatifs aux personnes faisant l'objet d'un suivi par le maire dans le cadre de ses missions de prévention de la délinquance ».

Cette autorisation unique encadre uniquement les traitements mis en œuvre dans le cadre du fonctionnement des groupes relevant directement des pouvoirs du maire en la matière comme les conseils locaux de sécurité et de prévention de la délinquance (CLSPD) et les conseils pour les droits et devoirs des familles (CDDF).

Pour les traitements concernés, la délibération de la CNIL précise les finalités exactes qui peuvent être poursuivies et les utilisations qui doivent être exclues, notamment l'alimentation d'autres traitements locaux ou de fichiers nationaux.

Elle établit une liste limitative des données qui peuvent être collectées dans le cadre de ces fichiers et prévoit des conditions supplémentaires pour le traitement de certaines données sensibles du point de vue de la protection des données personnelles.

Elle liste également les seules personnes habilitées à connaître des informations collectées dans le cadre de la

prévention de la délinquance, en distinguant les personnels pouvant disposer d'un accès direct aux traitements mis en œuvre, des personnes à qui ces informations peuvent être communiquées, pour certaines de manière ponctuelle uniquement.

L'autorisation unique n° AU-38 prévoit enfin une durée de conservation limitée, des modalités particulières d'information des personnes concernées ainsi que des mesures de sécurité adaptées à la sensibilité des traitements mis en œuvre.

Délib. CNIL n° 2014-262, 26 juin 2014, JO 22 juill. ; Site de la CNIL

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/124981/Default.aspx

---

Les objets connectés à notre e-santé dévoilent nos données

personnelles

Les objets connectés à notre e-santé dévoilent nos données personnelles

Alors que la présence du wearable (ensemble des vêtements et accessoires comportant des éléments informatiques et électroniques avancés) croît rapidement et avec elle, la collecte d'informations de santé, la Commission fédérale du commerce américain s'inquiète de ce que peuvent devenir ces données très personnelles.

Samsung a SAMI, Apple a Healthkit Google a Google Fit.

Trois grands noms des smartphones et trois approches de l'e-santé qui ont pour point commun de recueillir, formaliser et stocker vos données de santé sur votre téléphone ou sur des serveurs.

Quoi de plus personnel que votre état de santé et ses indicateurs ? Quoi de plus précieux et éventuellement de plus valorisés pour fournir des services complémentaires ?

Julie Brill, commissaire au sein de la Commission fédérale du commerce (FTC) s'inquiétait en tout cas de l'accélération de cette tendance qui va prendre encore plus d'importance avec la multiplication des montres et bracelets connectés. Pour elle, la façon dont les données sont « siphonnées » par ces applications est préoccupante. « Nous ne savons pas où ces informations vont en définitive », indiquait-t-elle devant un groupe de discussion organisé par le site politique The Hill. « Cela met les consommateurs dans une situation inconfortable », continuait-elle. La Commissaire a souligné devant le Congrès l'importance de voter une loi pour interdire la collecte d'informations personnelles sous de faux prétextes.

Le besoin de régulation ?

En mai dernier, la FTC rendait un rapport dans lequel elle indiquait qu'une bonne part des développeurs d'applications d'e-santé donnait accès aux données de santé collectées à des sociétés extérieures. Ainsi, l'étude menée sur douze applications de fitness et e-santé démontrait que ces informations électriques étaient partagées avec 76 entreprises différentes, y compris pour du marketing.

Face à un paysage si inquiétant et totalement dépourvu de cadre légal, la commissaire de la FTC s'inquiète que « personne ne parle de nouvelle réglementation ».

L'ACT, Association for Competitive Technology, lobby qui défend les intérêts des développeurs d'applications, craint évidemment qu'une quelconque réglementation nuise à l'innovation. Morgan Reed, directeur exécutif de l'ACT, déclarait ainsi à l'occasion de ce groupe de discussion : « L'industrie de la santé mobile a besoin d'éduquer la FTC sur les apports positifs que peut avoir la collecte d'informations sur la santé. […] Si nous échouons dans ce rôle, la commission pourrait prendre des décisions qui pourraient dévaster les

développeurs d’applications ».

Ci-dessous à la 34ème minute, Julie Brill, commissaire au sein de la Commission fédérale du commerce.

http://www.ustream.tv/recorded/50427445

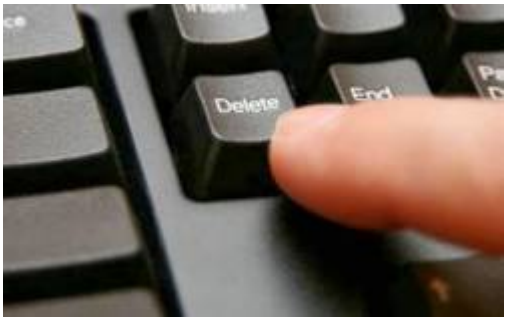
Si les bénéfices de la surveillance régulière de notre santé sont indéniables, il va une fois encore faire attention à ne pas devenir un produit dans la stratégie marketing d’acteurs peu soucieux de nos vies privées. Pour éviter ces pièges, Julie Brill préconise qu’un gros effort pédagogique soit fourni, d’une part et d’autre part que les utilisateurs soient toujours informés des informations recueillies et partagées. Un effort de transparence pour les plus personnelles de nos données…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.01net.com/editorial/624302/e-sante-debut-de-la-bataille-pour-nos-donnees-entre-la-ftc-et-les-lobbies/#?xtor=EPR-1-NL-01net-Actus-20140724

Suppression de données sur Google, découvrez la procédure à suivre…



Suppression de données sur Google, découvrez la procédure à suivre…
Rappelez-vous le mois dernier, la Cour de Justice de l'Union Européenne avait tranché sur le fait que Google devait désormais désindexer des contenus.
La procédure peut enfin démarrer.
Découvrez la procédure à suivre :

Suppression de données sur Google, découvrez la procédure à suivre…

Le mois dernier, je vous informais au travers de cet article : « Supprimer ses données sur Google ? Le droit à l'oubli a de la mémoire » que la Cour de Justice de l'Union Européenne avait tranché sur le fait que Google devait désormais désindexer des contenus à la demande d'individus concernés.

Un nombre incalculable de résultats de recherche apparaissent dans le célèbre moteur de recherche Google, mais il n'était malheureusement pas possible de demander la suppression de certains résultats jusqu'alors.

Suite à une décision de la Cour de Justice de l'Union Européenne en faveur du droit à l'oubli, vous aurez désormais la possibilité de demander la suppression de certains

résultats sous condition.

Pour mettre en oeuvre le dispositif, Google propose un formulaire en ligne à destination des Européens, permettant d'indiquer les liens jugés obsolètes, hors de propos ou inappropriés. Une décision importante qui lève de nombreuses questions : quels seront les critères utilisés pour savoir si le lien sera effectivement supprimé ou non ? Sous combien de temps le lien sera-t-il supprimé ? Bien que cette décision soit en faveur des internautes, elle donne également un grand pouvoir de décision au géant de Mountain View.

Attention, 24h après la mise en route de ce service, plus de 12 000 formulaires ont été complétés et envoyé à Google. « Nous évaluerons chaque demande individuelle et tenterons de trouver un juste équilibre entre la protection de la vie privée des individus et le droit du public à accéder à ces informations et à les diffuser. » Explique Google

Accès au formulaire

Vous devrez renseigner

– votre Nom,

– le Nom complet associé aux résultats de recherche à supprimer,

– votre relation avec la personne que vous représentez, si ce n'est vous-même,

– votre adresse e-mail de contact,

– les liens associés à votre nom et que vous souhaitez voir supprimés

Vous aurez besoin d'une copie d'une pièce d'identité avec

photo en cours de validité pour remplir ce formulaire.

Pendant que des millions de sociétés se cassent la tête à apparaître le mieux possible dans les résultats de recherches sur Google, d'autres se battent pour y disparaître…

A mon avis, il devrait y avoir rapidement plusieurs millions de demandes d'effacement de données dans les index de Google. Le géant du Net va t-il embaucher ? quel profil va se charger de traiter ces demandes ? En combien de temps ces demandes seront traitées ?
Et enfin, peut-on laisser Google décider du sort de nos données et être seul à juger de la pertinence de nos demandes ?

De nombreuses questions vont rester longtemps en suspens…

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Références :

05/06/2014 : http://www.zdnet.fr/actualites/droit-a-l-oubli-peut-on-faire-confiance-a-google-pour-decider-du-sort-de-nos-donnees-39802029.htm

02/06/2014 : http://www.zdnet.fr/actualites/droit-a-l-oubli-entre-casse-t

ete-pour-google-et-inquietudes-39801819.htm

02/06/2014
: http://www.zdnet.fr/actualites/droit-a-l-oubli-google-a-deja-recu-pres-de-12-000-demandes-39801777.htm

30/05/2014
: http://www.weblife.fr/breves/google-suppression-de-resultats-de-recherche-a-la-demande

---

La France nome un chef de la protection des données personnelles pour les administrations – CDO Chief Data Officer

	**La France nome un chef de la protection des données personnelles pour les administrations** La ministre de la fonction publique – de la décentralisation et de la réforme de l'Etat –, Marylise Lebranchu, a annoncé la création en France du poste d'administrateur général des données, également baptisé CDO ou « chief data officer » par les anglophones.

La France nome un chef de la protection des données personnelles pour les administrations

La ministre de la fonction publique – de la décentralisation et de la réforme de l'Etat –, Marylise Lebranchu, a annoncé la création en France du poste d'administrateur général des données, également baptisé CDO ou « chief data officer » par les anglophones.

Encore peu nombreux dans le monde à occuper cette fonction en entreprise, ce CDO a pour mission de coordonner l'utilisation des données, dans un contexte de transformation numérique où de plus en plus de données sont générées – mais souvent trop rarement exploitées.

La France est le premier pays européen à créer la fonction d'administrateur des données ou CDO. Ce poste est confié à Henri Verdier, patron d'Etalab. Il aura pour mission de développer la culture de la donnée dans les administrations et de favoriser la circulation des données.

L'administration française disposera donc de ce profil. Et cette fonction s'inscrit dans le cadre de la politique du gouvernement en faveur de l'open data ou partage de données publiques. Un domaine dans lequel la France se veut une référence en Europe.

Marylise Lebranchu compte sur ce « chief data officer » pour accélérer l'ouverture des données et contribuer « à élaborer une pratique interministérielle d'utilisation des données ». Ce poste a été confié au patron d'Etalab, Henri Verdier, qui coordonne la stratégie open data en France.

Mais pour agir réellement sur la culture des administrations française, cet administrateur devra être doté de pouvoirs. A

ce titre, la ministre de la fonction publique précise ainsi qu'Henri Verdier sera « autorisé à connaître les données détenues par l'administration de l'État et ses opérateurs ».

Plus largement, le premier CDO français aura pour mission d'organiser, en respectant la vie privée, « une meilleure circulation des données dans l'économie comme au sein de l'administration », de « veiller à la production ou à l'acquisition de données essentielles », de lancer des expérimentations et de développer une culture (ainsi que des outils et méthodes) de la donnée au sein des administrations.

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Références :

http://fr.wikipedia.org/wiki/Chief_Data_Officer

http://www.zdnet.fr/actualites/la-france-se-dote-d-un-chief-data-officer-39801427.htm

Supprimer ses données sur Google ? Le droit à l’oubli a de la mémoire

Supprimer ses données sur Google ? Le droit à l’oubli a de la mémoire

La Cour de Justice de l’Union Européenne a tranché. Google doit désindexer des contenus à la demande d’individus concernés.

Le droit à l’oubli a de la mémoire

La Cour de Justice de l’Union Européenne a tranché. Google doit désindexer des contenus à la demande d’individus concernés. Mais le droit à l’oubli doit s’appliquer au cas par cas, notamment pour des informations ayant trait à la vie publique.

Un particulier espagnol, nommé Mario Costeja González, avait saisi la CJUE (Cour de Justice de l’Union Européenne) en 2009 afin d’exiger de Google désindexe de son moteur des contenus le concernant. Il s’agissait d’informations publiées par un quotidien concernant une saisie immobilière l’ayant frappé pour recouvrement de dette.

Après avoir réglé sa dette, l’homme considérait alors que cette mention devait disparaître des arcanes du Web. Il saisi alors la CNIL espagnole afin que ces contenus soient effacés

des archives du journal mais aussi de Google. Ce qu'on appelle le droit à l'oubli.

L'Agence Espagnole de Protection des Données (AEPD), l'équivalent de notre CNIL mais en Espagne, ordonne alors de Google d'exécuter ces demandes. Mais le moteur refuse et entame une procédure devant la justice espagnole qui elle même se retourne vers la CJUE pour trancher.

Et l'avis de la CJUE est sans appel et risque de bouleverser les indexations d'informations concernant les individus :

Google doit proposer aux internautes la possibilité de désindexer des résultats de recherche les concernant.

Pour les observateurs, cette décision de la CJUE constitue une surprise. En effet, elle va à l'encontre de l'avis de l'avocat général qui avait considéré que Google n'était pas responsable des données personnelles indexées dans son moteur, annulant de fait les demandes de droit à l'oubli.

Rappelons que le droit à l'oubli numérique est défini de la manière suivante par la Commission européenne dans son projet de règlement :

« Toute personne devrait avoir le droit de faire rectifier des données à caractère personnel la concernant, et disposer d'un « droit à l'oubli numérique » lorsque la conservation de ces données n'est pas conforme au présent règlement. En

particulier, les personnes concernées devraient avoir le droit d'obtenir que leurs données soient effacées et ne soient plus traitées, lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été recueillies ou traitées, lorsque les personnes concernées ont retiré leur consentement au traitement ou lorsqu'elles s'opposent au traitement de données à caractère personnel les concernant ou encore, lorsque le traitement de leurs données à caractère personnel n'est pas conforme au présent règlement. »

Affaire à suivre…

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Références :

16/05/2014 Droit à l'oubli dans Google : le début des excès ?

14/05/2014 Droit à l'oubli : Google « déçu » de l'arrêt de la justice européenne

13/05/2014 Europe : Google doit proposer un droit à l'oubli aux internautes

20/06/2013 L'UE soutient la Cnil et l'Espagne lance à son tour une procédure contre Google

Détection de virus en ligne, Antimalwares et Antivirus Online

Ce n’est pas parce que votre ordinateur fonctionne correctement qu’il n’est pas infecté.

En effet, que ça soit dans les ordinateurs, les téléphones portables, les smartphones et même les tablettes, de plus en plus de virus ou de logiciels espions fonctionnent dans l’ombre. Leur principale fonction est d’espionner ce que vous tapez au clavier ou ce que vos logiciels envoient sur le réseau interne, wifi ou internet.

Ces logiciels recherchent, mémorisent et peuvent envoyer à un serveur pour un usage ultérieur :

Mots de passe saisis au clavier, envoyés sur le réseau filaire ou Wifi
Numéros de carte bancaire saisis au clavier, envoyés sur le réseau filaire ou Wifi
Carnet d’adresse pour contaminer vos contacts en utilisant votre identification pour tromper la confiance des interlocuteurs
Besoin de détecter si votre ordinateur est infecté par un virus sans installer d’antivirus ou désinstaller votre antivirus actuel ?

Pages Jaunes perd face à la CNIL

Pages Jaunes perd face à la CNIL

Constatant que Pages Jaunes avait récupéré les données personnelles de dizaines de millions d'utilisateurs sur les réseaux sociaux, la CNIL lui avait adressé en 2011 un avertissement. Le 11/04/2014, le Conseil d'Etat vient de confirmer, pour la deuxième fois, cet avertissement.

Pages Jaunes perd face à la CNIL

Constatant que Pages Jaunes avait récupéré les données personnelles de dizaines de millions d'utilisateurs sur les réseaux sociaux, la CNIL lui avait adressé un avertissement. Le Conseil d'Etat vient de confirmer ce deuxième avertissement. Etape suivante, la condamnation….

En septembre 2011, la CNIL avait averti Solocal Group (anciennement Pages Jaunes) car elle avait aspiré environ 34 millions de profils » sur différents réseaux sociaux (Facebook, Twitter, Viadeo, Copain d'avant, etc…).

La CNIL dénonçait alors une « collecte déloyale », puisque les internautes n'étaient pas informés que leurs données personnelles étaient susceptibles d'être aspirées puis mises en ligne sur le site des pages blanches. De plus, elle faisait valoir un droit d'opposition difficile à exercer.

Septembre 2011 : Pages jaunes averti par la CNIL. Pages jaunes saisit le Conseil d'Etat.

Mars 2012 : Rejet parle Conseil d'état de la Question Prioritaire de Constitutionnalité introduite par Pages jaunes

Avril 2014 : Le Conseil d'état confirme sa position, rejete la demande d'annulation de l'avertissement et condamne Pages Jaunes

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Références :

14/04/2014 http://www.linformaticien.com/actualites/id/32815/donnees-personnelles-la-cnil-gagne-contre-les-pages-jaunes.aspx

13/04/2014 http://www.commentcamarche.net/news/5864394-cnil-la-justice-confirme-la-condamnation-des-pagesjaunes-pour-vol-de-donnees

11/04/2014 http://lexpansion.lexpress.fr/high-tech/pages-jaunes-perd-contre-la-cnil_1507931.html

23/09/2011 http://lexpansion.lexpress.fr/high-tech/la-cnil-rappelle-a-l-ordre-pages-jaunes_1377597.html#xtor=AL-189

La CNIL peut maintenant effectuer des contrôles à distance

	La CNIL peut maintenant effectuer des contrôles à distance de sites Internet. Jusqu'ici les contrôles étaient effectués dans les entreprises, ou bien grâce à des documents et des fichiers fournis par les entreprises, ou bien aussi en convoquant les responsables concernés.

Jusqu'à maintenant, la CNIL pouvait exercer ses missions de contrôle des traitement de données personnelles soit :

– sur place (serveurs, ordinateurs, applications)

– sur pièce (à partir de documents ou de fichiers sur demande)

– sur audition (par convocation dans les locaux de la CNIL

La loi n° 2014-344 du 17 mars 2014 vient compléter les moyens qu'à la CNIL pour exercer ses mission.

La CNIL aura désormais la possibilité de réaliser ses CONTRÔLES EN LIGNE.

Elle pourra ainsi effectuer des contrôles à distance des sites internet, à partir d'un ordinateur connecté à Internet,

constater le non respect de la loi Informatique et Libertés et dresser un procès verbal qui sera opposable aux contrevenants.

Une précision tout de même pour vous rassurer : Un communiqué de la CNIL précise tout de même que la nouvelle loi « ne donnera évidemment pas la possibilité à la Cnil de forcer les mesures de sécurité mise en place pour pénétrer dans un système d'information ».

Source : Denis JACOPINI et cnil.fr

Références : Sur le site de la CNIL
http://www.cnil.fr/linstitution/actualite/article/article/un-pouvoir-dinvestigation-renforce-grace-aux-controles-en-ligne/

La loi n° 2014-344 du 17 mars 2014
http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000028738036

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)