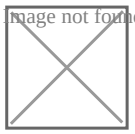
Image not found or type unknown



ANONYMAT SUR INTERNET :USAGES DE VOS DONNEES PERSONELLES

publié le **22/06/2016**, vu **3114 fois**, Auteur : Murielle Cahen

Avec le développement des activités numériques sur le web, le terme « anonyme » prend une nouvelle orientation. Ainsi, des millions d'internautes naviguent sur le web de façon anonyme, du moins le croient-ils, en consultant des sites d'information ou d'e-commerce. Dans le même temps, d'autres millions d'internautes ont ouvert des comptes personnels sur des réseaux sociaux en se cachant derrière un pseudonyme. Alors qu'on utilise de plus en plus Internet, qu'on y laisse toujours plus de données et qu'il est de plus en plus facile de savoir qui y fait quoi, l'inquiétude quant a? l'utilisation de ces données grandit chaque jour.

En toute hypothèse, sur le web, la sensation d'anonymat est décuplée par la distance qui existe entre l'internaute et le serveur auquel il accède pour y consulter des informations ou pour y créer des données (donner une opinion, écrire un texte, uploader un document, etc.). Et la sensation d'anonymat s'accroit chez de nombreux internautes à partir du moment où ils se cachent derrière un écran et un pseudonyme.

Dans la pratique, moins de 5% des internautes mettent en place des pratiques d'offuscation de leurs traces sur le web. A contrario, cela signifie que plus de 95% des internautes vivent avec une sensation d'anonymat alors même qu'ils ne sont pas anonymes sur Internet.

On notera le caractère ambigu de l'anonymat : d'un côté, c'est ce qui est sans nom, sans valeur, parfois menaçant ; de l'autre, c'est une stratégie de protection, de préservation, porteuse d'égalité (dans le cas par exemple, de l'anonymat du vote en France). Cette dualité se retrouve également sur internet.

I. L'anonymat, principe nécessaire à la protection de la vie privée sur internet

A. Anonymat et vie privée sur internet

Anonymat et vie privée sont très souvent associés, et pour cause. Le premier est un moyen de préserver la seconde. La vie privée est la raison pour laquelle on peut recourir à des techniques d'anonymisation. Internet bouleverse la manière dont nous gérons notre vie privée.

La vie privée ne peut se comprendre qu'en termes de contrôle de ce qu'on laisse sur internet. Elle consiste à conserver le contrôle d'une information personnelle et ne pas la laisser sortir d'un cadre dans lequel elle a été rendue publique.

Sur internet, l'utilisateur ne laisse pas seulement des traces volontairement et de manière visible. S'il existe bien des traces visibles et intentionnelles (commentaire sur un blog, photo sur les réseaux sociaux), les traces invisibles et non intentionnelles sont d'autant plus nombreuses (l'adresse IP quand on se connecte à un site internet, requête dans les archives d'un moteur de recherche). Il y a également les cookies placés sur le navigateur ou le tracker, qui est un petit programme présent sur les sites web qui enregistre certaines activités à des fins publicitaires, présent sur les sites de e-commerce.

L'historique de connexions et de visites, l'adresse IP, les recherches Google, les favoris et l'historique complet, les emails : ceux sont autant d'informations qui peuvent être collectées sur internet :

B. L'encadrement juridique de la protection des données collectées sur internet

En France, la CNIL, la Commission nationale informatique et libertés veille à ce que loi Informatique et libertés de 1978 et les autres textes qui protègent ces données personnelles, soient respectés, afin d'éviter les abus et les atteintes aux droits fondamentaux.

S'il est aisé d'imaginer que nous sommes tous fichés par l'Etat et les organismes qui lui sont rattachés (sécurité sociale, fisc, police à travers la carte nationale d'identité, la préfecture lors de l'établissement de la carte grise, le Pôle emploi, le médecin, etc.), par son employeur, par des associations indépendantes (club de sport, association à laquelle on fait un don, forum de discussion ou chat, etc.) ou encore par des sociétés commerciales (banque, assureurs, téléphonie, fichiers clients des commerces, etc.), on imagine moins être fichés par des sociétés que l'on ne connaît pas. Et pourtant, les données personnelles circulent facilement soit contre rémunération pour le titulaire du fichier, soit de manière involontaire en cas notamment de piratage informatique ou de détournement de la finalité d'un fichier.

En 2014, la CNIL affirme que près de 35% des recruteurs avouent avoir déjà écarté un candidat à un emploi à cause d'une e-réputation négative.

En France, le texte fondateur en matière de protection des données est la Loi informatique et liberté du 6 janvier 1978 qui définit les principes à respecter lors de la collecte, du traitement et de la conservation des données personnelles. Elle renforce les droits des personnes sur leurs données, prévoit une simplification des formalités administratives déclaratives et précise les pouvoirs de contrôle et de sanction de la CNIL.

La loi "Informatique et Libertés" est applicable dès lors qu'il existe un traitement automatisé ou un fichier manuel, c'est-à-dire un fichier informatique ou un fichier « papier » contenant des informations personnelles relatives à des personnes physiques.

II. L'anonymat, principe menacé par les développements technologiques

A. Le Big Data au détriment de l'anonymat

Copyright © 2025 Légavox.fr - Tous droits réservés

Littéralement, le terme de « Big Data » signifie mégadonnées, grosses données ou encore données massives. Ils désignent un ensemble très volumineux de données qu'aucun outil classique de gestion de base de données ou de gestion de l'information ne peut vraiment travailler. En effet, nous procréons environ 2,5 trillions d'octets de données tous les jours. Ce sont les informations provenant de partout : messages que nous nous envoyons, vidéos que nous publions, informations climatiques, signaux GPS, enregistrements transactionnels d'achats en ligne et bien d'autres encore. Ces données sont baptisées Big Data ou volumes massifs de données. Les géants du Web, au premier rang desquels Yahoo (mais aussi Facebook et Google), ont été les tous premiers à déployer ce type de technologie.

L'analyse des données est capable d'extraire des informations très précises sur les individus en croisant des données anonymes. Par exemple, les signaux de géolocalisation des portables, la démarche d'un passant filmée par vidéosurveillance, le choix de films téléchargés forment autant d'indicateurs sur les habitudes, les intérêts et les activités des personnes.

Actuellement, la tendance est à la convergence des différentes données disponibles. Data en ligne et hors ligne, structurées ou non structurées rassemblées et consolidées, accord entre Facebook et des courtiers de données : les algorithmes n'ont pas fini de générer de plus en plus de sources lucratives sur le marché des Big Data. Plus encore : il est possible de prédire où se trouvera une personne d'ici 80 semaines sur la base de données de géolocalisation issues de son GPS. Finalement, rester non identifié devient une gageure.

B. Une pression croissante de l'État

Depuis une dizaine d'années, les initiatives de la part des gouvernements pour tenter de réguler et de contrôler internet se sont multipliées. Rappelons les révélations d'Edward Snowden en 2013, qui ont montré que les collectes massives d'informations par la NSA, concernant des citoyens du monde entier, dépassaient le cadre de la lutte nécessaire contre le terrorisme ou contre les autres risques géopolitiques.

La France n'est pas en reste, puisque son service de renseignement extérieur, la DGSE (Direction Générale de la Sécurité Extérieure), a également à sa disposition un système d'interception massif d'Internet, sans compter sa proximité avec l'opérateur Orange. Au delà des services de renseignement, ces dernières années, le législateur français a été particulièrement attentif à la régulation d'internet : LCEN (loi pour la confiance en l'économie numérique) ; DADVSI (loi relative aux droits d'auteur et droits voisins dans la société d'information) , LOPPSI 2 (loi d'orientation et de programmation pour la performance de la sécurité intérieure), Hadopi (loi Création et Internet de la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet) ou encore les lois antiterroristes qui accroissent la surveillance du réseau à la recherche de potentiels terroristes. Cette pression croissante des gouvernements à des fins de contrôle, de régulation et de surveillance peut se faire au détriment de l'anonymat des utilisateurs d'internet.

Le 15 novembre 2001, la France a adopté la loi sur la sécurité quotidienne, dont l'article 29 oblige les fournisseurs d'accès à internet à conserver les identifiants de connexion de leurs abonnés. Ses mesures, dont l'article 29, auraient dû arriver à expiration fin décembre 2003. Cependant un amendement de la loi sur la sécurité intérieure du 21 janvier 2003, a pérennisé les mesures de conservation des identifiants et les a séparées du motif terroriste, leur raison d'être de l'adoption de la première loi. Ces mesures sont désormais présentes dans l'article 34-1 du code des postes de communications électroniques.

À partir de la loi de 2004 et de la loi pour la confiance en l'économie numérique, la conservation des identifiants de connexion, qui devait être effectuée uniquement par les opérateurs de télécommunications, donc les fournisseurs d'accès à internet, concerne également les

Copyright © 2025 Legavox.fr - Tous droits réservés

hébergeurs, c'est à dire, tous les sites qui mettent à disposition du public un service de « stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature » (sites d'informations, services de vidéo type Dailymotion ou Youtube, Wikipédia…). Le décret précisant les modalités n'est intervenu que le 1er mars 2012.

Le 1er mars 2016, le ministre des Finances Michel Sapin a annoncé que le gouvernement va mettre fin à l'anonymat des cartes bancaires prépayées, utilisées dans la préparation des attentats du 13 novembre, afin de lutter contre le financement du terrorisme. La veille, dans le cadre de la loi sur la réforme de la procédure pénale, Eric Ciotti, député Les Républicains, a déposé un amendement visant à forcer le déchiffrement des smartphones dans les enquêtes antiterroristes. Sous peine d'interdiction de la commercialisation de ces outils.

Sources :

http://www.dcc-marketing.com/2015/02/lanonymat-cest-quoi/

http://www.net-iris.fr/veille-juridique/dossier/20679/les-donnees-personnelles-et-la-protection-de-la-vie-privee-a-heure-des-nouvelles-technologies.php

http://www.cil.cnrs.fr/CIL/spip.php?rubrique281

https://books.google.fr/books?id=zSsTBQAAQBAJ&pg=PR18&lpg=PR18&dq=anonymat+sur+internet+mé
Tqbi1hwnlvMc&hl=fr&sa=X&ved=0ahUKEwjksqHopafLAhUGVxoKHWTYAggQ6AEIOTAF#v=onepage&q=

http://www.journaldunet.com/ebusiness/le-net/1169618-vers-un-reglement-europeen-sur-la-protection-des-donnees-qui-vise-les-plateformes-us/

http://www.zdnet.fr/actualites/etat-d-urgence-le-gouvernement-n-interdira-pas-le-wi-fi-public-et-tor-39829552.htm

http://rue89.nouvelobs.com/blog/oh-my-code/2016/03/05/respect-de-la-vie-privee-apple-ou-surveillance-generalisee-fbi-vous-de-choisir-235245

Copyright © 2025 Légavox.fr - Tous droits réservés