

Le fait du jour

Internet : vers la revanc

DONNÉES PERSONNELLES Jusqu'ici, la protection sur la Toile des informations personnelles relevait plutôt du problème de l'internaute. Un nouveau règlement européen pourrait tout changer en mai

PASCAL RABILLER
p.rabiller@sudouest.fr

C'est bien pratique, il faut le reconnaître, de renseigner une fois pour toutes ses coordonnées bancaires sur un site marchand. C'est tellement plus facile de cocher « J'ai bien lu les conditions » sans les lire quand on veut installer un nouveau système d'exploitation ou booster les outils de recherche du mobile, du PC ou de la tablette en surfant sur le Wi-Fi public. Souvent, nous sacrifions la maîtrise minimale de nos

données, voire de notre sécurité, sur l'autel de l'économie de notre consommation d'énergie et de forfait, parfois par paresse. La plupart du temps, c'est d'abord pour gagner du temps que nous sommes laxistes sur le sujet. Et ce temps que nous ne voulons pas sacrifier, de très nombreuses entreprises qui nous fournissent des services ou des produits, le transforment en argent.

L'argent des données personnelles est devenu un des principaux modèles économiques de beaucoup d'acteurs du Net. L'argent des données personnelles est devenu un des principaux modèles économiques de beaucoup d'acteurs de la Toile. À commencer par les géants américains ou chinois du Net, qui disposent des habitudes de « clics » et de consommation, des centres d'intérêt et des déplacements géolocalisés de milliards d'internautes. Nos données ont un prix, entre 10 centimes et 1 euro, en fonction du nombre d'informations personnelles fournies (âge, lieu de résidence, sexe, situation familiale, adresse IP...) en plus du seul mail. C'est souvent à notre corps défendant que nous livrons certains des moments de notre vie privée au plus grand nombre, et pas juste à nos amis. Tout ce qui a été publié un jour, même effacé par la suite, continue de vivre dans les couloirs des réseaux sociaux et constitue, pour les as de la recherche, notre véritable identité numérique.

Algorithmes et mégadonnées

Quel internaute sait que quand il pousse les portes virtuelles d'un magasin comme Cdiscount ou Amazon, il est accompagné, tout aussi virtuellement, de dizaines de logiciels espions « vendeurs » d'autres boutiques concurrentes, qui analysent ses recherches, ses centres d'intérêt, et qui, ô miracle, proposent un bien ou service du même acabit ? Pas de magie

en réalité, mais des algorithmes et des analyses de mégadonnées. Ces derniers se basent sur des informations que nous avons soit dévoilées volontairement, soit, et c'est plus généralement le cas, parce que nous n'avons pas la maîtrise des outils qui nous permettent de dire stop. Ceux-ci existent pourtant, puisque les utilisations de données informatiques sont encadrées en France depuis le 6 janvier 1978 et en Europe depuis 1995.

Certes, la protection de nos données nous appartient encore, elle est relative à nos comportements, mais, à partir du 25 mai prochain, demain donc, nous, e-consommateurs européens, allons indirectement disposer d'un outil qui va nous permettre, à tout moment, d'accéder aux données personnelles que les acteurs détiennent. Le Règlement général pour la protection des données (RGPD) va ainsi harmoniser la gestion des informations personnelles dans l'ensemble des pays de l'Union européenne.

La donnée, source de revenu ?

Il concerne l'ensemble des acteurs présents sur le Net, organismes publics, associations, entreprises européennes, mais aussi des sociétés dont le siège est hors de l'Union européenne et qui traitent de données relatives à des citoyens de celle-ci. À partir de mai 2018, nous aurons tous plus de visibilité et de contrôle sur nos données

personnelles. Depuis l'annonce du calendrier, c'est le branle-bas de combat du côté des acteurs, qui doivent savoir en permanence quelles informations ils détiennent et, surtout, savoir les transmettre sur simple demande.

Le RGPD (ou GDPR, en anglais) est une manne pour les entreprises de services numériques, de conseils et les cabinets d'avocats qui doivent aider les acteurs concernés à se mettre en conformité. On parle ici d'un marché à 4,3 milliards d'euros entre la période 2017 et 2021. Ce contrôle plus aisé de nos données pourrait avoir un impact sur la commercialisation de celles-ci par les internautes aux sociétés qui les utilisent pour générer des revenus publicitaires. Lancée par le philosophe Gaspard Koenig, cette idée n'a pas été trop mal accueillie par les acteurs d'Internet. De là à dire qu'une autre révolution de la donnée personnelle, mieux contrôlée cette fois, est en cours...



Les utilisations de données informatiques sont encadrées en France depuis le 6 janvier 1978 et en Europe depuis 1995. PHOTO ILLUSTRATION THIERRY DAVID / « SUD OUEST »

« Les objets connectés sont tr

CYBERSÉCURITÉ Faiblement protégés pour ne pas renchérir leur coût et souvent inventés par des start-up, les objets connectés sont des proies faciles

« Plus de 8 objets connectés sur 10 sont vulnérables face aux cyberattaques », explique Laurent Oudot, expert de la Direction générale de la sécurité extérieure (DGSE). Il dirige aujourd'hui la société Tehtris, à Pessac (33), qui a mis au point eGambit, l'une des 10 meilleures solutions au monde de protection des stations et des serveurs. C'est en effet un jeu d'enfant pour un pirate informatique de s'infiltrer dans un objet connecté en moins de trois minutes, selon un récent rapport du cabinet ForreScout. Un problème majeur au regard de la vitesse de déploiement des objets connectés dans nos foyers. En 2020, il devrait y en avoir 6 milliards dans l'Union européenne.

Des cas de piratages massifs

D'ailleurs, depuis deux ans, les coups à grande échelle se multiplient. Ainsi, en octobre 2016, des pirates ont

pris le contrôle de dizaines de milliers d'objets connectés pour mener des attaques par déni de service [NDLR : saturation de sites par des millions de requêtes simultanées], contre l'hébergeur tricolore OVH ou la société Dyn (un annuaire du Web), perturbant fortement des services aussi divers que Twitter, Spotify ou Amazon.

Les conséquences peuvent être particulièrement graves. En juillet 2015, deux chercheurs en sécurité ont démontré qu'ils pouvaient s'infiltrer dans le système connecté d'une voiture et en prendre le contrôle à distance. Des pirates peuvent aussi potentiellement ruiner une entreprise en s'introduisant dans le système connecté de chauffage pour mettre en surchauffe physique tous ses serveurs et réduire toutes les données à néant. Les raisons de ces failles sont bien connues. « Ces objets connectés

sont, pour la plupart, créés par des start-up, qui veulent accéder le plus vite possible au marché avec des prix accessibles et font des économies sur la sécurité, en ne prévoyant souvent ni mots de passe cryptés, ni mises à jour. Ils sont bien trop vulnérables pour les pirates », pointe cet expert.

Des espions cachés

Certaines sociétés étrangères, peu scrupuleuses, n'hésitent pas à profiter de ces faiblesses pour détourner des objets connectés à des fins d'espionnage. Ainsi, la poupée interactive Cayla, fabriquée par Genesis Industries Limited, une entreprise de Hongkong, collecte moult informations personnelles relatives à l'enfant : son prénom, son école, son adresse, ses émissions préférées... sans que l'on sache l'usage qui en est fait ensuite. L'Allemagne a clairement choisi d'en interdire la vente.

he de la vie privée ?



Et si Google avait des raisons d'avoir peur du français Qwant ?

STRATÉGIE Le moteur de recherche français Qwant est un pionnier de la protection des données

« Quand nous nous sommes lancés, en 2010, beaucoup nous disaient que notre militantisme ne servait à rien, que nous n'y arriverions pas... » Éric Léandri est un militant un peu particulier. Son engagement est celui d'un geek, qui a décidé, au moment où Google devenait ce qu'il est aujourd'hui - un « aspirateur » à données personnelles qu'il transforme en machines à cash tous azimuts -, de prendre le contre-pied avec un moteur de recherche respectueux de la vie privée de ses utilisateurs.

Qwant, seul au monde ?

Il est, avec quatre autres ingénieurs informaticiens, à l'origine de Qwant, le seul moteur de recherche européen qui garantit la non-exploitation des données personnelles. « Peut-être même le seul au monde, car, si aux États-Unis, un autre acteur, DuckDuckGo, assure être sur la même longueur d'onde que nous, il s'agit en fait d'un métamoteur de recherche. C'est-à-dire qu'il est un intermédiaire entre les internautes et les moteurs de recherche du marché. Et puis, dans un environnement juridique qui est quand même beaucoup plus laxiste que le nôtre, je ne suis pas certain que nous ayons la même notion du respect des données personnelles », glisse le dirigeant.

Si au moment de sa création, Qwant semblait pour beaucoup à contre-courant des tendances, les vents sont en train de tourner. « Pendant longtemps, tout le monde se

moquait du respect des données personnelles. On avait confiance quand on nous disait que c'était avec nos données que les services s'amélioreraient. Et on nous garantissait la sécurité... Le futur règlement général sur la protection des données, le RGPD, et les nombreux problèmes de protection des données personnelles des internautes qui ont émaillé l'actualité ces dernières années, font de ce thème un vrai sujet de société. Il nous rend, tout d'un coup, très tendance », constate Éric Léandri, qui a été de la délégation française qui a accompagné le président Emmanuel Macron en Chine, la semaine dernière.

« Le Google d'avant 2010 »

Les chiffres d'utilisation de Qwant lui donnent raison. Le moteur de recherche compte désormais chaque mois plus de 52 millions de requêtes. Un chiffre qui plafonnait à 1 million en 2014 et qui est actuellement en croissance de 10 à 20 % chaque mois. En quelques semaines, les équipes de Qwant - réparties entre Nice, Milan, Paris, Berlin et bientôt la Chine - sont passées de 50 à 140 collaborateurs. Dont près d'une vingtaine se consacrent uniquement au sujet du respect des données personnelles des utilisateurs.

Éric Léandri réagit instantanément quand on lui pose la question d'une éventuelle incompatibilité entre la « philosophie » de Qwant et le business. « C'est faux ! Avant 2010, Google n'exploitait pas les données person-



Éric Léandri, fondateur et dirigeant de Qwant. PHOTO DR

nelles comme c'est le cas aujourd'hui. Pourtant, il faisait déjà 40 milliards de dollars de chiffre d'affaires ! Qwant, c'est le Google d'avant 2010 », assure Éric Léandri. Ce « Google d'avant » devrait, lui, réaliser 10 millions de chiffre d'affaires cette année, ce qui lui permettra d'atteindre l'équilibre financier. Selon l'Ifop, Qwant accueille actuellement 4 % des recherches en France. S'il n'y a que huit moteurs de recherche dans le monde, le français veut devenir la référence dans le domaine de la protection des données. P. R.

op faciles à pirater »



La poupée interactive Cayla collecte ainsi moult informations personnelles relatives à l'enfant. PHOTO DR

Surtout, le problème est qu'actuellement, les consommateurs n'ont guère de solutions sûres à 100 % pour se protéger. Juste des conseils de bon sens : privilégier de grandes marques reconnues, faire les mises à jour régulièrement ou encore utiliser un routeur pour sécuriser sa connexion

Internet. Le sujet est tellement sensible que la Commission européenne va définir, cette année, des mesures visant à imposer aux objets connectés des normes standards de cybersécurité et à développer des dispositifs de certification.

Nicolas César

Ces données personnelles qui nous échappent

Les cookies

Ils sont déposés sur l'ordinateur lors de chaque visite d'un site Web. Ils peuvent stocker les données de navigation mais également des informations personnelles sur les sites marchands pour « tracer » l'activité des internautes et personnaliser l'affichage des messages publicitaires.



Les réseaux sociaux

Les paramètres de confidentialité sont rarement configurés par les utilisateurs de Facebook. Ils permettent pourtant à des tiers d'accéder à de nombreuses informations personnelles, aux profils des contacts d'un utilisateur ou à son identité.



La géolocalisation

Sur ordinateur ou depuis un téléphone, elle est généralement activée par défaut. Elle permet aux annonceurs d'adresser des offres commerciales ciblées selon la position de l'utilisateur ou de suivre ses déplacements, même lorsqu'une application est en veille.



Le numéro de carte bancaire

Certaines boutiques en ligne proposent de les stocker pour simplifier la commande. Au risque qu'une faille sur leurs serveurs ou un piratage de données entraîne leur réutilisation frauduleuse.

