Que deviennent nos données personnelles sur Internet?

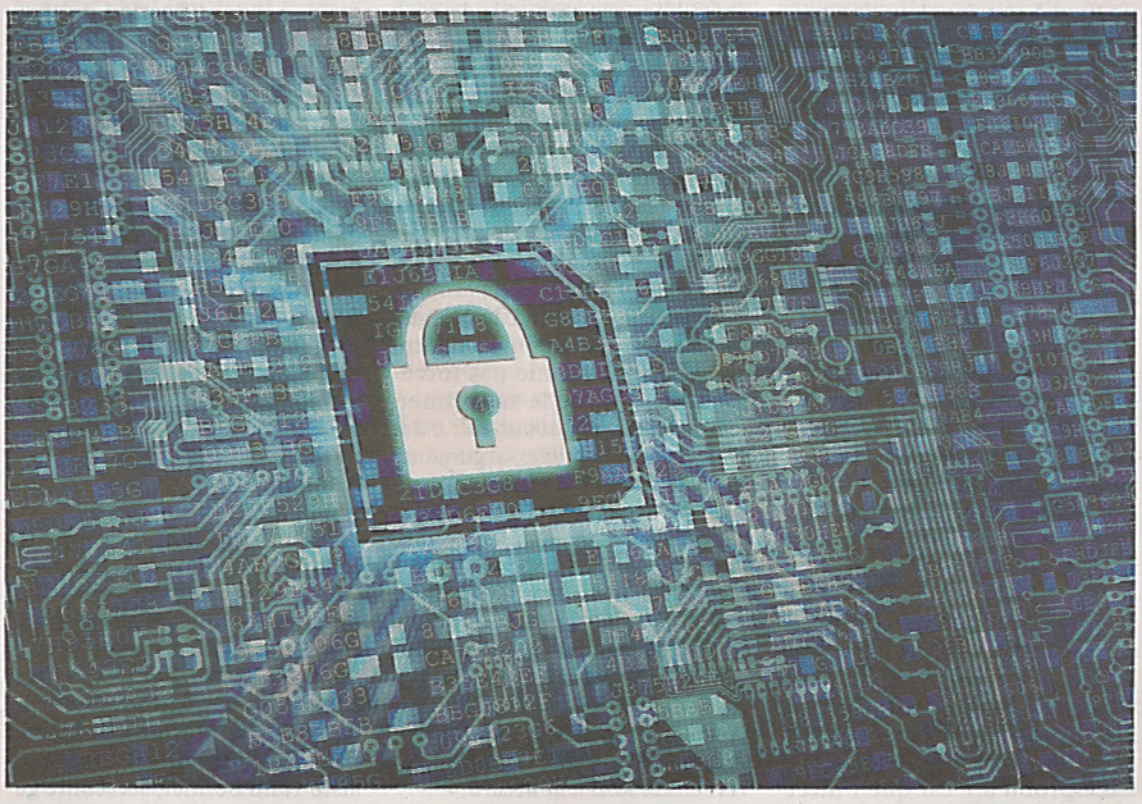
La création d'un fichier regroupant les données personnelles des Français pose la question plus large de l'utilisation des données collectées sur Internet.

Devant l'ordinateur, les yeux font des allers-retours rapides. Chiffre après chiffre, de la carte bleue au clavier à l'écran. Chaque jour, des millions de Français transmettent des informations sur un site Internet. Numéro de carte bancaire, nom, adresse, âge, mais aussi données de navigation, heures de connexion... La quantité de données personnelles renseignées sur Internet dépasse l'imagination.

« *Les données personnelles peuvent être explicitement fournies par l'internaute ou récupérées de façon implicite*, explique Serge Abiteboul, professeur à l'ENS Cachan et membre de l'Académie des sciences. *Des informations qui nous concernent sont créées par des programmes au cours de la navigation.* » Un peu comme quand votre banquier étudiait votre attitude en plus de votre dossier pour vous accorder un prêt. Sauf que votre banquier a été remplacé par des algorithmes et que votre attitude est enregistrée, au même titre que votre dossier.

« *Une fois collectées sur un ordinateur, les données personnelles voyagent jusque dans le serveur d'une entreprise* », raconte Serge Abiteboul. C'est là que les choses se compliquent. Se pose d'abord la question de l'emplacement géographique du stockage. Contrairement à l'image populaire d'un « nuage » qui flotterait on ne sait où, les données sont toujours physiquement stockées quelque part. Et cela peut être en France, en Europe ou dans n'importe quel pays du monde. Impossible pour l'utilisateur de le savoir, et impossible de savoir quelle législation s'applique à ces informations.

Bruno Rasle, délégué général de l'Association française des correspondants aux données personnelles (AFCDP), se veut rassurant. « *Actuellement, si les données sont en France ou dans n'importe quel pays de l'Union européenne, la législation européenne s'applique*, explique-t-il. *Les données ne peuvent sortir de l'UE qu'après autorisation de la Cnil (Commission nationale informatique et libertés).* »



Il est impossible de savoir où sont stockées les données numériques des utilisateurs d'Internet. *Nmedia-Fotolia*

Outre le lieu de stockage se pose ensuite la question du cryptage. N'importe quelle personne mal intentionnée peut-elle utiliser des données conservées? « *En France aujourd'hui, la plupart des données personnelles ne sont pas chiffrées, à l'exception des mots de passe* », explique Bruno Rasle. « *Les données peuvent être cryptées lors du trajet, mais pas lorsqu'elles sont stockées à un bout ou l'autre*, tempère Serge Abiteboul. *On souhaite juste éviter l'interception par un tiers malveillant.* » De fait, peu de vols de données ont lieu lors du transport. Contrairement au monde physique, il est plus facile de braquer la banque que d'attaquer le convoi de transport de fonds.

C'est du côté de l'internaute ou des serveurs que se concentrent les piratages.

C'est donc du côté de l'internaute ou des serveurs que se concentrent les piratages. Pour l'internaute, un antivirus et de bonnes pratiques permettent d'éviter bien des désagréments (*lire les repères*). Pour l'entreprise, le vol a en général lieu lorsque des pirates informatiques trouvent une faille dans un site Internet et peuvent remonter jusqu'à la base de données. Autre possibilité, des employés copient la base de données pour la revendre au plus offrant. Cette pratique ne date pas d'Internet, nuance Patrick Valduriez, directeur de recherche à l'Inria. « *Le vol de données confidentielles et l'espionnage ont toujours existé, même si les données numériques sont plus faciles à revendre et à diffuser.* »

Au-delà du piratage reste la question de l'utilisation légitime des données personnelles. « *L'utilisation la plus commune est l'envoi de publicité ciblée à l'utilisateur* », explique Serge Abiteboul. C'est l'exemple typique où après réservation d'un billet de train pour Rouen, toutes les publicités affichées concernent des hôtels à Rouen.

« *Mais ce qui peut être plus angoissant, c'est que parfois ces données collectées ne sont pas utilisées*

Suite page 14. ●●●

Que deviennent nos données personnelles sur Internet?

« Les messages d'internautes qui disent "je n'autorise pas Facebook à utiliser mes données personnelles" n'ont aucune valeur juridique. »

Le centre de serveurs (datacenter) de Facebook implanté à Lulea, en Suède. David Levene/eyevine/Bureau233

●●● *Suite de la page 13.*

par l'entreprise elle-même, poursuit l'académicien. *Vos données personnelles peuvent être vendues sur des places de marché à d'autres entreprises avec lesquelles vous n'êtes pas en contact. »* C'est notamment le cas des sites qui proposent des services gratuits, comme Facebook. Le réseau social n'est pas payant et ne vend pas de produits, il doit donc trouver un moyen de se rémunérer : en vendant des informations personnelles.

« Une donnée personnelle n'appartient pas à l'individu, elle le concerne. »

« Utiliser un service c'est en accepter toutes les clauses, rappelle Patrick Valduriez. *Les messages d'internautes qui disent "je n'autorise pas Facebook à utiliser mes données personnelles" n'ont aucune valeur juridique. Si vous utilisez Facebook, vous acceptez que l'entreprise utilise vos informations comme elle le souhaite. » « Une donnée personnelle n'appartient pas à l'individu, elle le concerne,* appuie Serge Abiteboul. *Il ne faut pas croire que ces informations servent à espionner les utilisateurs ; dans la plupart des cas, il s'agit surtout de faire du business et les informations échangées sont de qualité assez médiocre ou obsolètes. »*

Le problème est que l'internaute est peu au fait de l'utilisation de ses informations personnelles. Pourtant, *« dès la loi informatique et libertés de 1978, il existait une obligation d'informer les personnes de la collecte de leurs données,* explique Bruno Rasle. *Mais ces indications sont trop souvent reléguées aux mentions légales alors que c'est quand on me demande mon nom et mon adresse qu'on devrait me dire pourquoi on les collecte et ce qu'on va en faire. »*

En attendant, reste la possibilité de demander. N'importe quel internaute peut obliger l'entreprise à lui communiquer les informations dont elle dispose sur lui dans les deux mois. *« C'est un droit que tout citoyen a, mais que peu utilisent »,* déplore le délégué de l'AFCDP. Attention, connaître son profil ne donne pas forcément le droit de le supprimer. *« Autrement cela aboutirait à des situations impossibles,* argumente Bruno Rasle. *Vous pourriez écrire à la direction des impôts pour supprimer toutes les informations vous concernant et échapper à l'impôt. »*

« Sans compter que beaucoup d'internautes sont contents d'obtenir de meilleurs services grâce à leurs données personnelles, analyse Serge Abiteboul, *ils préféreraient juste qu'elles ne soient pas revendues sans leur accord. »*

Audrey Dufour

repères

Pour plus de sécurité :

Vérifier la sécurité d'un site Internet. Un petit cadenas en haut à gauche et un lien qui commence par « https » signifient que la page est sécurisée. Si elle ne l'est pas, ne surtout pas communiquer d'informations sensibles.

Ne pas donner d'informations par courriel. Le *phishing* (ou hameçonnage) est une pratique où un pirate se fait passer pour une entreprise pour demander des mots de passe ou des numéros de compte. Les entreprises dont vous êtes client n'ont pas besoin que vous leur communiquiez des informations personnelles par courriel.

TES, un mégafichier controversé?

La création d'un fichier regroupant les données personnelles des Français, défendue par le gouvernement au nom de la lutte contre les fraudes, est contestée en raison des risques pour les libertés publiques.

TES, pour « Titres électroniques sécurisés ». Derrière cet acronyme, c'est le projet d'un immense fichier, qui doit rassembler les données biométriques – identité, couleur des yeux, domicile, photo, empreinte digitale – de près de 60 millions de Français. Du jamais-vu ! L'objectif est de réunir les détenteurs d'un passeport et d'une carte d'identité en un seul fichier. Mais ses détracteurs – la Commission nationale informatique et libertés (Cnil) en tête – ont affiché leur crainte pour les libertés publiques. Au ministère de l'intérieur, on assure qu'en aucun cas le fichier ne pourra servir à l'identification des personnes. TES, explique le gouvernement, doit élargir le fichier qui existe déjà pour les passeports biométriques aux cartes d'identité, et est donc un moyen de lutte contre la fraude documentaire.

TES a fait l'objet d'un décret du gouvernement paru au *Journal officiel* le 30 octobre. Décision trop rapide ? *« Cela n'a jamais été fait, et je crois que cela nécessite un débat au Parlement »,* a souligné Isabelle Falque-Pierrotin, présidente de la Cnil. Même réaction de la part du Conseil national du numérique (CNNum) qui souligne une certaine *« précipitation »* gouvernementale. Cette instance consultative a appelé à la suspension de TES et s'est autosaisie pour examiner des alternatives. Son avis est attendu mi-décembre. *« Nous souhaitons montrer qu'il n'y a pas un seul choix possible pour atteindre ces objectifs, et que celui qui a été fait a des conséquences éthiques »,* insiste Yann Bonnet, secrétaire général du CNNum.

Les possibles détournements du fichier inquiètent. *« TES, c'est beaucoup de bruit pour rien,* réagit Philippe Goujon, député LR. *Il est nécessaire pour lutter contre le terrorisme et je voudrais même que ses finalités aillent plus loin. Qu'il permette l'authentification et l'identification. »* Cet outil est indispensable pour lutter contre la fraude et le terrorisme, renchérit Jean-Luc Taltavull, secrétaire général adjoint du Syndicat des commissaires de la police nationale. *« Les cartes d'identité font l'objet de nombreux trafics. Et l'éparpillement des données ne permet pas de repérer une usurpation d'identité. »*

« Il faudra être prudent afin de le protéger contre toute tentative de piratage extérieur », insiste-t-il néanmoins. Une telle base attise forcément des convoitises, et en informatique le risque zéro n'existe pas. Pour répondre à ces inquiétudes, le ministre de l'intérieur, Bernard Cazeneuve, a fait appel à l'ANSSI, qui travaille à la sécurisation des systèmes d'information. L'agence, au service du premier ministre, donnera un « avis conforme » sur la sécurité de cette base de données.

Des solutions plus sûres existent-elles ? Les détracteurs de TES défendent une solution décentralisée : inscrire les données biométriques sur une puce embarquée dans la carte d'identité. *« Intégrer les données personnelles de chacun à une telle puce – plutôt que de les agréger dans un fichier centralisé – permettrait aux citoyens d'en garder la maîtrise »,* explique Marc Rees, spécialiste du droit des nouvelles technologies et rédacteur en chef de *NextInpact.*

Aujourd'hui, TES est testé dans les Yvelines. Les auditions se poursuivent au Parlement, et le gouvernement attend les conclusions des experts. Si le décret doit évoluer, le texte devra repasser devant la Cnil et le Conseil d'État. Soit plusieurs mois à attendre avant tout changement législatif.

Frédérique Schneider