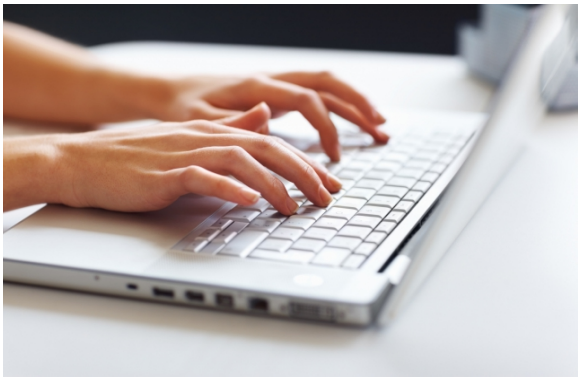
Sécuriser ses données: une responsabilité partagée

21.05.2015 15:45
Par Florence Thibaut

Surveiller sa e-réputation, nettoyer les traces de son passage en ligne, déterminer qui a accès à ses métadonnées sont autant de défis pour protéger son identité numérique. Pour atténuer les risques, on peut recourir à un browser moins connu, à un coffre-fort numérique pour ses mots de passe ou encore encapsuler ses données.



Protéger sa e-réputation devient de plus en plus compliqué.

Tentatives de harponnage, attaques malveillantes, usurpation d'identité, vol de mots de passe ou utilisation de données à des fins commerciales: les pièges qui attendent les internautes non avisés sont nombreux. Avec la démocratisation des objets connectés, l'explosion des réseaux sociaux et le succès des applications géolocalisées, ces risques, globalisés et difficilement identifiables, ne feront qu'augmenter.

Face à ces ennemis sans visage, il est, toutefois, possible de réagir, notamment en connaissant ses droits et en étant conscient de l'existence de métadonnées, soit les données liées aux données, qu'on sème tous à travers le web. Avec 98% des ménages luxembourgeois connectés, 60% des citoyens sur les réseaux sociaux et 74% qui achètent régulièrement en ligne, la problématique concerne bien tout le monde.

Tous visés

C'est ce qui a amené Axa Luxembourg(http://www.axa.lu) à donner une conférence sur ce sujet dans les locaux flambant neufs de Nyuko, illustrant bien les changements à l'œuvre dans nos manières de travailler et de diffuser l'information. «Avec la facilité d'utilisation des technologies, le principal danger est que les utilisateurs se rendent très peu compte de l'usage fait de leurs informations personnelles, y compris de leurs données bancaires ou mêmes de leurs appels téléphoniques. Certains livrent des informations qu'ils ne diffuseraient jamais dans 'la vraie vie'. Il ne faut pas croire que cela n'arrive qu'aux autres! Nous sommes suivis partout», cadre Olivier Vansteelandt, CIO d'Axa, qui a récemment ajouté une protection numérique à son offre Optihome pour les particuliers. «En tant que directeur informatique, le faire comprendre est un combat quotidien. On n'a jamais autant parlé de sécurité dans les départements IT.»

Pour aller plus loin dans la pédagogie, l'assureur vient de mettre en ligne un «Guide du bon sens numérique (https://www.axaprevention.fr/conseils-internet/risques-internet-bon-sens-numerique)», avec des conseils pratiques pour les internautes. «En 2014, il y a eu 317 millions de malwares, le danger est bien réel», alerte Philippe Dambly, juriste de formation et product manager au sein de la société Lar (http://www.lar.be/fr) (Legal Assistance & Recovery). «La difficulté est que ces nouveaux risques sont globaux et itératifs, ils évoluent en fonction de la technologie. À côté des outils, il y a surtout des relations humaines et des utilisateurs. Plus qu'une réponse technique à apporter, je crois beaucoup en la sensibilisation.» Des coffres-forts électroniques, des «sand box» pour éviter les virus ou des réseaux VPN privés sont autant de moyens de limiter son exposition.

Réflexes à adopter

Pour Jan Guth, étudiant en informatique et président du Chaos Computer Club (http://wiki.c3l.lu/doku.php?id=projects:bigbrother.lu), un groupe de hackers «éthiques» et activistes créé en 2008, c'est d'abord à ces fameuses métadonnées, véritable ombre numérique, qu'il faut faire attention. «Dans chaque document Word, par exemple, différentes informations sont conservées, de la date de création du

fichier à son auteur. La même logique s'applique aux photos qui comportent de nombreux éléments, y compris des coordonnées GPS», explique-t-il. «Sans paramétrage adéquat, toutes ces données peuvent se retrouver sur le web. Ce n'est plus de la science-fiction, mais une réalité. Il suffit de voir ce que des géants comme Apple ou Google conservent comme données sur leurs utilisateurs pour s'en convaincre. Avec un smartphone, tout trajet peut être retracé facilement, ce qui permet un profilage très précis.»

Si pour la Cour de justice européenne et son homologue américaine la US Court of Appeal, il est officiellement illégal de conserver ces données, dans la pratique, les exemples de brèches sont légion.

Pour se débarrasser de ses traces numériques, plusieurs options sont possibles. Le président du Chaos Computer Club recommande ainsi l'utilisation du navigateur Tor (https://www.torproject.org/projects/torbrowser.html.en), spécialement conçu pour une navigation confidentielle, plutôt que des grands noms comme Safari ou Internet Explorer. «En utilisant différents relais intermédiaires, il anonymise l'échange d'informations et rend l'espionnage plus compliqué pour les services de renseignement, les sociétés commerciales ou les États non démocratiques», affirme Jan Guth. «Ensuite, le recours au MAT(https://mat.boum.org/), Metadata Anonymisation Toolkit, permet d'effacer les données attachées à ses photos, documents ou autres formats.»

Cadre fluctuant

Vivement discuté, le projet de règlement européen sur la protection des données actuellement à l'étude au Parlement européen a déjà fait l'objet de 4.000 amendements, illustrant bien toute la complexité du sujet. Pour Emmanuelle Ragot, partner à l'étude Wildgen et spécialiste des nouvelles technologies, c'est tout un changement de paradigme qu'il induit. «Il permettra de passer d'un exercice de compliance a posteriori, statique et passif, à un modèle de gouvernance plus proactif et reposant sur un modèle de 'privacy by design', soit dès le départ.» Les sanctions ont également été durcies. On parle déjà d'amendes potentielles allant jusqu'à 5% du chiffre d'affaires ou 100 millions d'euros.

Directement applicable comme tout règlement européen, le texte pourrait être adopté à la fin de l'année 2015, potentiellement sous l'égide de la présidence européenne. Tournant dans la protection des internautes, il étendra certaines notions importantes comme le droit à l'oubli numérique, au déréférencement ou la gestion du consentement.

Au Luxembourg, depuis la loi du 18 juillet 2014 sur la cybercriminalité, la «clé digitale», soit toutes les informations permettant d'identifier une personne en ligne, est en outre un bien protégeable contre le vol et la contrefaçon. «De cette matière, il y a toujours un équilibre et un compromis à trouver entre accélération des flux transfrontaliers et protection des consommateurs. Il y a une solide volonté politique autour du marché unique digital qui est en jeu, il ne faut pas l'oublier. C'est aussi un des points à l'agenda du TTIP», rappelle Me Ragot.