PROTECTION DES DONNÉES: Un luxe ?

Von Luc Caregari | 2013-08-02 |Medien

Alors que le monde entier commence à se faire à l'idée qu'il faudra mieux protéger ses données, le Luxembourg ne semble pas trop se soucier des nouveaux enjeux. Un retard qui risque de coûter très cher.

La prochaine fois que vous croisez un flyer comme celui-ci, pensez à y aller. Car l'internet, c'est comme le sexe : mieux vaut avoir des rapports protégés.

Depuis ce jeudi matin, les terminologies « Prism » ou « Tempora » sont devenues un peu plus obsolètes. Car il y a bien pire. Comme vient de le révéler le « whistleblower » – toujours bloqué à l'aéroport de Moscou – Edward Snowden, l'arme ultime de la NSA s'appelle « XKeyscore ». Depuis 2008, ce programme permet aux services de renseignement américains d'accéder à toute information sur le net, sans limitations. De plus, des filtres leurs donnent aussi la possibilité d'encercler des « activités suspectes ». Vous vous trouvez dans un pays arabe et vous communiquez en français ou en allemand ? Bing ! Une petite lampe rouge s'allume dans un bureau secret aux States. Même si le vice-ministre de la justice américain James M. Cole a immédiatement assuré que les services américains n'iraient pas jusqu'à enregistrer des noms, des contenus ou des adresses, la confiance dans de telles allégations est morte depuis longtemps. Au point où même des députés républicains commencent à questionner le bien-fondé de tels programmes, même si le gouvernement leur assure qu'il aurait su déjouer des douzaines d'attentats, grâce à l'utilisation de ces métadonnées.

Et que se passe-t-il au Luxembourg au même moment ? Rien, ou pas grand-chose. Avec un ministre de l'économie qui assure aux consommateurs qu'ils pourront de toute façon continuer à télécharger « au noir », un scandale d'espionnage intérieur et politique qui ne scandalise vraiment que ses victimes. Voir aussi la révélation jeudi matin de la radio 100,7 selon laquelle les partis politiques – même déi Lénk –

utiliseraient les données personnelles pour mieux cibler leurs électeurs personnels pour leurs campagnes électorales – le pays donne une piètre image de sa conscience des temps qui courent. Surtout s'il essaie de se reconvertir dans le cyberbusiness, une perspective affichée par tous les partis au pouvoir. Mais on peut douter que l'infrastructure en place soit vraiment prête pour une telle évolution. Une anecdote pour preuve : lorsque le ministre des Finances Luc Frieden a présenté il y a deux semaines en grandes pompes le projet « Lux-Ict », ses services avaient tout simplement ommis de réserver l'URL www.luxict.lu à temps. En d'autres mots : le monde de l'internet évolue avec une telle rapidité que le Luxembourg ne peut pas se permettre son retard habituel de cinq à dix ans. C'est « Innovate or Die », comme disait l'ancien ministre de l'économie Jeannot Krecké.

« Innovate or Die »

Pourtant, même au grand-duché il y a des villages gaulois qui tentent d'organiser la résistance en rendant le public conscient des dangers des mondes virtuels. Cela se passe par exemple dans le sous-sol du café Konrad à Luxembourg-Ville, qui, pour mieux rendre l'atmosphère, ressemble à une vraie crypte avec son plafond voûté. Il s'agit de la sixième « Cryptoparty » organisée par le Chaos Computer Club et Hackerspace.lu – deux organisations qui depuis des années représentent la communauté internationale des hackers au Luxembourg. Mais lors du dernier rendez-vous, qui a eu lieu le 25 juillet, les choses étaient un peu différentes. Non pas qu'il y ait eu une affluence de masse dans la cave du café Konrad – on n'en est pas encore là – mais du moins, une équipe de la télé RTL était venue filmer l'événement. La preuve que la cryptographie – donc le fait d'encoder ses données sur internet pour éviter de se faire espionner par qui que ce soit – est en train de devenir de plus en plus populaire au Luxembourg aussi.

Le programme présenté essentiellement lors de cette « Cryptoparty » répond au doux nom de « Tor Project ». Originalement conçu par l'« U.S. Naval Research Laboratory », il est aujourd'hui utilisé par tous ceux qui souhaitent, pour une raison ou pour une autre, encrypter leurs données. Un de leurs principaux représentants n'est autre que Jacob Appelbaum, un « hacker » dont on entend parler de plus en plus dans les médias. En effet, son engagement pour Wikileaks lui a déjà valu des ennuis avec la justice américaine, qui a même obtenu les clés de son compte Twitter.

Comment ça fonctionne ? « Tor Project » est à la base un réseau de tunnels virtuels qui permet aux personnes qui les utilisent de communiquer de façon anonyme. Sur le site www.torproject.org, tout un chacun peut télécharger un programme qui rend anonyme ses connections – que ce soit dans les recherches effectuées sur le net, dans les courriels ou dans les chatrooms. De plus, on peut aussi télécharger sur le site des programmes pour préconfigurer ses clés USB ou CDs afin de les rendre plus sûrs, un programme pour encrypter son smartphone (malheureusement, Orbot ne fonctionne que sur les smartphones configurés sous Android) ou encore un navigateur Tor – qui est amélioré en permanence. Donc, en somme un paquet pour se protéger dans – presque – toutes les situations encourues sur internet. Et gratuit en plus – même si le « Tor Project » vit aussi de donations.

Mais est-ce que cela vous protège vraiment de tomber dans les mailles d'un service secret ? C'était un des points les plus intéressants de la discussion à la dernière « Cryptoparty ». Parce que si vous encryptez vos communications, les services secrets ne peuvent, probablement, pas accéder à vos contenus. Pourtant, ils peuvent savoir que c'est vous qui encryptez vos communications. Ce qui vous rend suspect d'office. Comme quoi, on est encore loin du meilleur des mondes possibles?