

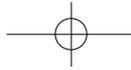
Édito

Big Brother, le retour

Dans sa première vie (sous la forme de magazine), *Terminal* a agité le spectre de Big Brother débouchant sur un nouveau totalitarisme entraîné par le développement de l'informatisation tous azimuts de la société. Puis progressivement, nous nous sommes laissés convaincre que cette menace était exagérée, voire imaginaire, et que le danger réel était dans la multiplication des « little brother », dans le contrôle social qu'ils instituaient insidieusement, dans l'exhibition de toutes et tous sur les réseaux sociaux ou dans les techniques de management des grandes entreprises.

Déjà en 1996, les révélations sur le réseau d'espionnage des réseaux satellitaires de communication Échelon mis en place par un certain nombre de pays dont les États-Unis et la Grande-Bretagne avaient soulevé quelques questions en Europe : le Parlement européen demanda des rapports sur l'existence d'Échelon, ainsi que sur les moyens techniques et juridiques qui pourraient être utilisés pour la protection des données personnelles en Europe. Mais après les attentats du World Trade Center, ces rapports ont vite été enterrés et s'installa assez rapidement une collaboration entre les services secrets des pays occidentaux pour une surveillance accrue de tous les moyens de communication au nom de la lutte contre le terrorisme.

Les États-Unis l'instituèrent, sous la présidence de Georges W. Bush, par le vote du Patriot Act qui fut prorogé par l'administration Obama, malgré les déclarations faites par celui-ci lors de sa campagne électorale. Dans l'émotion suscitée par cette attaque sur le sol des États-Unis, les citoyens américains acceptèrent dans leur large majorité cette surveillance digne du livre « 1984 » et les pleins pouvoirs donnés aux services de sécurité. Cela se fit plus discrètement dans les pays européens (Grande-Bretagne, Allemagne, France...) et les citoyens n'en furent informés que lorsqu'Edward Snowden révéla au grand jour l'existence du programme PRISM et des autres programmes de surveillance des données circulant sur Internet. Au nom de la lutte contre le terrorisme, la NSA imposa la possibilité pour ses services d'accéder aux informations (mails, vidéos, photos, blogs) enregistrées sur les serveurs de neuf grandes entreprises de l'Internet dont Google, Microsoft,



Yahoo, Apple, Skype, AOL... Dans le même temps, on apprenait que grâce au GCHQ (Government Communications Headquarters) anglais, les méta-données¹ sur les communications Internet et téléphoniques circulant sur les fibres transatlantiques entre la Grande-Bretagne et les États-Unis étaient récupérées, ce qui permettait de cartographier les échanges entre les USA et l'Europe.

En résumé, Échelon est étendu à tout l'Internet et cette fois avec accès au contenu des échanges en cas de besoin en intervenant directement sur les serveurs des entreprises. Et l'Europe est évidemment en première ligne car les services de Google, Microsoft, Apple et évidemment le réseau social Facebook sont d'un usage courant dans les pays européens. Chaque pays européen joue sa propre partition dans ce concert d'espionnage : le Royaume-Uni comme meilleur allié, une fois encore, des États-Unis, fournissant l'aide logistique pour la surveillance des liaisons transatlantiques, les services allemands acheminant toutes leurs informations à leurs confrères américains, la France essayant selon ses moyens de bâtir son propre réseau tricolore².

Nos pires pressentiments quand, dans les années soixante-dix, certains³ alertaient sur les dangers potentiels de l'informatique au service des États et des grandes administrations, se sont vérifiés. La technologie informatique permet d'interconnecter toutes les informations émises par un individu ou par un groupe et de tracer la vie privée de chacun. La lutte contre un ennemi extérieur et intérieur, le terrorisme, justifiant par avance cette surveillance généralisée. Mais il n'en reste pas moins que cette fuite en avant vers une société totalitaire reste dans un flou juridique et politique comme si nos démocraties avaient du mal, même aux États-Unis, à assumer ces pratiques en opposition aux discours tenus par nos gouvernants sur la défense des libertés démocratiques et des droits de l'homme.

Quel espace reste-t-il pour ceux et celles qui ne se résignent pas à ce grignotage permanent de nos libertés ? Il est à noter que les CNILs européennes ont été également prises de cours en pleine discussion sur la réforme des institutions et des lois pour la protection des données personnelles par les révélations de l'affaire Edward Snowden.

La France qui se targue d'être toujours à la pointe du combat pour les droits de l'homme s'enorgueillirait de donner asile à ce « lanceur d'alerte » ou du moins, si nos accords diplomatiques avec les États-Unis nous en empê-

1. Adresses mails ou numéros de téléphones appelés, durée de l'appel, objet du mail.

2. Révélations sur le Big Brother français, *Le Monde*, 4 juillet 2013.

3. Safari ou la chasse aux français, Philippe Boucher, Louis Joinet, Philippe Lemoine. *Le Monde* 21 mars 1974.



chent, de reconnaître le rôle positif qu'il a joué dans la dénonciation des pratiques de surveillance par la NSA et les services secrets européens comme l'a fait le Groupe des Verts/ALE au Parlement européen en proposant Edward Snowden pour le Prix Sakharov 2013, prix annuel de l'Union européenne (UE) pour la « liberté de l'esprit » qui est décerné chaque année.

Du point de vue pratique, il est difficile de résister à la surveillance de masse instituée par la NSA. Les techniques cryptographiques sont une première réponse mais elles ne sont pas infaillibles et la NSA se vante de pouvoir décrypter, grâce à l'utilisation de superordinateurs une grande partie des documents (mails, bases de données d'entreprises ou de gouvernements amis ou ennemis) stockés dans ces puissantes machines. Un nouveau centre d'interception des télécommunications est en cours d'installation à Bluffdale au cœur de l'Utah⁴ avec un data center pouvant stocker cinq cents milliards de milliards de pages de texte. Selon Edward Snowden, la NSA entend enregistrer également non seulement les métadonnées des échanges sur l'Internet, mais également le contenu de ceux-ci. Toute cette information sera accessible à tous les services de sécurité US par des agents habilités. Un nouveau challenge s'ouvre pour les chercheurs en informatique : fournir à tous ceux qui le désirent (militant-e-s, responsables associatifs, gouvernements, entreprises) des solutions sécurisées utilisant les méthodes les plus avancées de la cryptographie pour décourager la surveillance dont ils sont l'objet quand ils utilisent les réseaux informatiques.

Même si on peut rêver comme Philippe Boucher, Louis Joinet et Philippe Lemoine⁵ d'une « Charte mondiale Informatique et Libertés », il faut profiter des réactions scandalisées dans de nombreux pays occidentaux aux révélations d'Edward Snowden pour clarifier les accords sur les échanges de données personnelles entre l'Europe et les États-Unis. Et imposer des solutions qui soient compatibles avec les lois Informatique et Libertés en vigueur dans de nombreux pays européens. Le débat sur ces questions doit sortir du cercle des spécialistes et être abordé au cours de la campagne des élections au Parlement européen l'année prochaine. ■

Jacques Vétois

4. Philippe Bernard, « Voyage au cœur de la NSA », *Le Monde* 29 août 2013

5. Affaire Snowden : la France reste muette, Philippe Boucher, Louis Joinet, Philippe Lemoine, *Le Monde*. 21 août 2013.