LE MONDE *diplomatique*

> **septembre 2013**, page 9

EN 1998, LA RÉVÉLATION DU SYSTÈME ECHELON CRÉAIT LA STUPÉFACTION

Espionnage électronique, quinze ans d'inertie

Annulation d'une rencontre entre M. Barack Obama et M. Vladimir Poutine, pressions du gouvernement britannique sur un journaliste du « Guardian » : les informations livrées par M. Edward Snowden sur le système d'espionnage électronique américain n'en finissent pas de faire des vagues. Quinze ans plus tôt, un scandale analogue avait éclaté sans que les gouvernements en tirent de conséquences pratiques.

PAR NICKY HAGER

INITIATEUR de l'une des fuites les plus retentissantes de notre époque, M. Edward Snowden restera dans l'histoire comme celui qui a révélé au monde la surveillance implacable et absolue qui s'exerce sur Internet. En l'espace d'une nuit, des mots comme « métadonnées » (informations sur les données personnelles) ou « Prism » (nom du programme de surveillance) sont entrés dans le langage courant.

Ce n'est pas la première fois que les « grandes oreilles » de l'Agence de sécurité nationale des Etats-Unis (National Security Agency, NSA) défraient la chronique. Il y a quinze ans, elles provoquaient déjà la consternation aux quatre coins du globe après la publication d'une étude du Parlement européen indiquant que *« toutes les communications électroniques, téléphoniques et par fax* [étaient] *quotidiennement interceptées* (1) ». Médusé, le grand public découvrait l'existence d'un programme de surveillance mondial baptisé « Echelon » (2). L'affaire fit les gros titres de la presse. On accusa le Royaume-Uni d'utiliser le Quartier général des communications du gouvernement (GCHQ) pour espionner ses voisins européens ; Microsoft fut mis en cause pour sa collaboration avec la NSA. L'affaire culmina avec la création par le Parlement européen d'une commission temporaire d'enquête.

L'existence d'Echelon avait été rendue publique dès 1988 par le journaliste britannique Duncan Campbell (3). Son article décrivait un dispositif capable de capter un nombre inouï de communications à travers le monde et de repérer à l'aide de mots-clés les messages susceptibles d'intéresser les services de renseignement : la surveillance à l'échelle industrielle. Paru en 1996, mon livre *Secret Power* prolongeait ce travail. Mais un article isolé et un ouvrage publié dans la lointaine Nouvelle-Zélande ne suffisent pas à retenir l'attention du grand public. C'est deux ans seulement après la parution du livre qu'un membre du Parlement européen relaya l'information et qu'Echelon fit irruption dans le débat public.

Une funeste coïncidence

Dans ses conclusions de 2001, la commission d'enquête sur Echelon avançait quelques propositions concrètes en vue de protéger l'Europe contre l'espionnage anglo-saxon. Les pays membres de l'Union européenne se voyaient notamment invités à *« promouvoir, développer et produire une technologie de chiffrement »* accessible à tous leurs citoyens et institutions (4). Le moment paraissait historique : pour la première fois se profilait une action politique d'envergure pour assurer la sauvegarde de la vie privée à l'ère de la surveillance globale. Mais cet espoir se brisa sur une funeste coïncidence : présenté au Parlement européen le 5 septembre 2001, le rapport final de la commission d'enquête fut balayé six jours plus tard par les attentats de New York et Washington.

Durant les années qui ont suivi, la surveillance a changé d'échelle. La guerre contre le terrorisme a optimisé les dispositifs de contrôle, mais les a aussi rendus — pour un temps — plus acceptables aux yeux du public. Douze ans après l'effondrement des tours jumelles, on en revient quasiment au point de départ. L'environnement politique d'aujourd'hui n'est pas sans points communs avec celui qui avait vu naître la polémique autour d'Echelon. Les preuves apportées par M. Snowden ont évidemment joué un rôle décisif ; leur révélation intervient de surcroît au moment propice, pour plusieurs raisons.

D'abord, une certaine inquiétude grandissait depuis quelque temps déjà chez les internautes au sujet de la surveillance de leurs réseaux. Ils manquaient toutefois d'éléments solides pour étayer leurs soupçons. La vie entière d'un individu étant désormais stockée électroniquement, toute intrusion dans ces données est potentiellement ravageuse. Mais comment réagir à ce viol virtuel s'il reste indécelable ?

La hantise d'autres WikiLeaks

A l'instant même où la technologie numérique nous offrait la Toile et les médias sociaux, elle mettait au point les instruments servant à moucharder leurs contenus. A l'époque des premiers textes sur Echelon, les techniciens du renseignement balbutiaient encore dans leurs efforts pour intercepter les courriels. Les capteurs d'Echelon ciblaient les communications par satellite et micro-ondes, mais, jusqu'à M. Snowden, le monde ne savait presque rien de la capacité des « grandes oreilles » à épier aussi les flots d'informations échangées sur Internet.

Echelon, puis Prism, cet « Echelon pour Internet », visaient essentiellement les communications de pays à pays. Mais, à l'époque déjà, le Federal Bureau of Investigations (FBI) pesait de tout son poids pour obtenir l'outillage technique et juridique nécessaire à l'espionnage des communications au sein d'un même territoire. Beaucoup de législations nationales contraignent désormais les opérateurs du Web et des télécoms à installer des portes dérobées dans leurs équipements et à laisser les agences de renseignement y accéder à leur guise. Les révélations de M. Snowden sur l'assistance fournie à la NSA par Gmail, Facebook ou Microsoft aident à comprendre ces « interceptions légales », pour reprendre le nom un brin oxymorique que leur a donné le législateur.

L'offensive antiterroriste constitue le deuxième facteur déterminant. L'exploitation des peurs sécuritaires a abouti à une explosion des budgets de renseignement et à une expansion illimitée des capacités de surveillance.

Le troisième ingrédient est aussi le plus crucial : le précédent WikiLeaks. L'association de M. Julian Assange a ancré dans l'opinion publique l'idée que faire fuiter sur la Toile des documents confidentiels constituait un moyen redoutable de contrer les excès et les abus du pouvoir ; que divulguer les secrets d'un Etat irrespectueux de la vie privée de ses citoyens pouvait ouvrir un espace à l'action démocratique. Les Etats-Unis, suivis par d'autres gouvernements, n'ont pas lésiné sur les moyens pour

dissuader quiconque de suivre l'exemple du « lanceur d'alerte » Bradley Manning, sans réussir à lui ôter son attractivité. En s'appuyant sur cet exemple, M. Snowden pourrait bien être en train de changer la donne.

NICKY HAGER
Journaliste, Wellington (Nouvelle-Zélande). Auteur de *Secret Power. New Zealand's Role in the International Spy Network* (Craig Potton Publishing, Nelson, Nouvelle-Zélande, 1996), le livre qui révéla l'existence du réseau Echelon.

(1) « An appraisal of technologies of political control [http://aei.pitt.edu/5538/1/5538.pdf] » (PDF), Scientific and Technological Options Assessment (STOA), Parlement européen, Strasbourg, 6 janvier 1998.

(2) Lire Philippe Rivière, « Le système Echelon [http://www.monde-diplomatique.fr/mav/46/RIVIERE/m1] », *Le Monde diplomatique,* juillet 1999.

(3) Duncan Campbell, « Somebody's listening [http://echelononline.free.fr/documents/dc/somebody_listening.htm] », *New Statesman,* Londres, 12 août 1988.

(4) « European Parliament resolution on the existence of a global system for the interception of private and commercial communications (Echelon interception system) [http://cryptome.org/echelon-ep-fin.htm] », 5 septembre 2001.

Mot clés: Internet Politique Terrorisme Technologie Électronique Services secrets Droit international Relations internationales Technologies de l'information États-Unis (affaires extérieures) États-Unis (affaires intérieures)