Echelon/Frenchelon : mythes et réalités

Enjeux politiques et stratégiques des systèmes de surveillance

Conférence de Jean Marc Manach, le 14 avril 2005
à l'IEP de Rennes à l'invitation de l'association YSEGORIA

Introduction

Le programme anglo-saxon d'écoute des télécommunications, surnommé « Echelon », qui fait de temps à autres les choux gras d'Hollywood et de certains jeux vidéos, et constitue l'un des sujets de prédilection des adeptes des « théories de la conspiration », est un « secret défense » plus ou moins battu en brèche par certains journalistes et défenseurs des droits de l'homme et de la vie privée.

« Frenchelon », son (relatif) équivalent français (et partiellement européen), est bien moins connu : révélée en 1998, son existence n'a jamais entraînée qu'une poignée d'articles de quelques journalistes (un anglais, cinq français), quand bien même plusieurs rapports parlementaires, et communiqués de presse du ministère de la Défense, en parlent à mots couverts.

Dans les deux cas, ils ne sont que la partie emergée d'un iceberg dont l'ampleur croît à mesure que se développe la société de l'information; la question reste en effet de savoir ce qui, de l'espionnage militaire (et politique, et industriel), ou de la surveillance administrative (et policière, et domestique), constitue la plus grande menace en termes de libertés, et de démocratie.

Chronique d'une médiatisation

1976 : un étudiant écossais en physique de 24 ans, Duncan Campbell, est arrêté par le contre-espionnage britannique pour avoir publié dans un journal (de gauche) une enquête sur une installation gouvernementale de surveillance électronique. S'ensuivent 18 mois de « tracasseries judiciaires », qui ne font que conforter Campbell dans son désir d'enquêter sur cette affaire.

1988 : grâce, entre autres, aux confessions d'une ingénieure qui a travaillé pour des sociétés privées sous contrat avec la National Security Agency américaine (NSA), Campbell, qui a délaissé la physique pour le journalisme d'investigation, révèle l'ampleur du programme anglo-saxon d'écoutes des télécommunications, que l'on surnomme depuis « Echelon ».

1999 : dans un rapport commandé le Parlement européen, et largement médiatisé, Campbell détaille l'histoire, le fonctionnement et l'évolution d'Echelon, et avance qu'en matière d'espionnage industriel, il rapporterait, chaque année, 25 milliards de dollars de contrats aux firmes américaines. Au détriment, essentiellement, de leurs concurrents européens ou japonais.

James Woolsey, ancien directeur de la CIA, reconnaît dans le WSJ l'existence d'Echelon et loue "*l'honnêteté intellectuelle*" de Campbell, qui précise que les USA justifient l'espionnage industriel par la lutte anti-corruption (cf les affaires Airbus et Thomson CSF), quand bien même l'écoute des négociations multilatérales, entre autres, relève quant à elle clairement de l'espionnage politique.

2001 : bien qu'elle n'ait pas anticipé les attentats du 11 septembre, et que la culture US du renseignement technologique s'en trouve sévèrement remise en question, la NSA est confortée dans ses missions, obtient plus de traducteurs, plus de moyens pour recruter plus de gens, et cherche aujourd'hui à gérer la sécurisation des réseaux informatiques de l'administration américaine.

2004 : après avoir autorisé la télévision à effectuer un reportage sur sa station d'écoute de Domme, l'armée française médiatise le lancement, en décembre, du satellite de renseignement par l'image Helios 2A -qui permet de différencier « un char d'un tracteur »- et des microsatellites Essaim de renseignement électromagnétique, deux des composantes de ce que l'on surnomme « Frenchelon ».

La guerre électronique, pendant militaire de l'explosion des « telcos »

1947 : les USA et la Grande-Bretagne, dans le cadre de l'alliance UKUSA (encore tenue secrète), mettent en place un système de surveillance des télécommunications du bloc de l'Est. Depuis, s'y sont ralliés le Canada, l'Australie et la Nouvelle-Zélande, ainsi qu'une dizaine d'autres pays, « sous contrat ». Dans tous les cas, c'est la NSA qui « traite » les données interceptées.

Sont concernés les signaux (SIGINT) et les communications (COMINT), qu'il s'agisse de communications radio, téléphoniques, fax, télex, mail, et plus généralement tout ce qui concourt aujourd'hui à l'internet, y compris lorsqu'ils transitent par des câbles subaquatiques ou des satellites : tout ce qui transite sur les réseaux de télécommunications est a priori écoutable.

Une multitude de filtres et d'agents logiciels, basés notamment sur des dictionnaires de mots-clés, des « signatures » (électroniques, vocales...) et des objectifs stratégiques concourrent à sélectionner ce qui doit, ou non, être traité par un agent humain (cf. le « Jam Echelon Day » qui, tout en contribuant à révéler l'existence d'Echelon, participa aussi des « théories de la conspiration »).

L'industrie des télécommunications participe elle aussi du développement d'Echelon : dernier avatar en date de cette alliance objective, la Hollande a ainsi récemment fait installer, aux côtés des radars (privés) dédiés aux communications civiles, des antennes chargées, précisément, d'écouter les télécommunications de ces mêmes radars...

Une trentaine de pays disposeraient de tels systèmes d'écoute des télécommunications, à ceci prêt que seule la France dispose, à l'instar des alliés du pacte UKUSA, de territoires -ses ex-colonies- répartis dans le monde entier, lui permettant d'écouter quelque communication que ce soit. Les anglo-saxons ont d'ailleurs, ironiquement, surnommé son programme « Frenchelon ».

Ces programmes d'espionnage, fonctionnant dans le plus grand secret et sans mandat judiciaire, sont bien évidemment illégaux : les USA avancent pour leur part qu'ils n'écoutent que les telcos des pays étrangers. Et si l'Angleterre n'est pas habilitée à espionner ses partenaires européens, et encore moins ses citoyens, on sait que Tatcher demanda à ses alliés d'espionner deux de ses ministres...

Vers une banalisation de l'espionnage domestique

Dans les années 90, la NSA, ses pairs et ses affidés, privés de communistes, se sont donc recylés, en partie, dans l'espionnage industriel. Non seulement pour ne pas perdre leur travail, d'autant qu'ils pouvaient aussi le faire pour le secteur privé (avec des salaires en conséquence), et que la « guerre économique » est devenue, pour les politiques, un enjeu géostratégique majeur.

Le développement industriel et technologique du Japon, et autres « dragons » du sud-est asiatique, a ainsi largement bénéficié de politiques, publiques, d'« intelligence économique ». Le renseignement (« intelligence », en anglais), a quant à lui, dans le même temps, été considérablement bouleversé par l'explosion des « sources ouvertes », grandement facilitée par le succès du web et de l'internet.

Pour en revenir à Echelon, Campbell avance ainsi que l'Advocacy Center, un organisme de soutien au commerce extérieur américain, vise aussi à permettre aux services de renseignement US, à commencer par la NSA, à faire bénéficier certaines entreprises privées, aux marchés et technologies sensibles, de leurs analyses et renseignements.

Pour en revenir à Frenchelon, Alain Juillet, qui fut PDG dans l'industrie agro-alimentaire avant d'être nommé n°2 de la DGSE en 2002, puis haut responsable chargé de l'intelligence économique en 2003, déclarait pour sa part que "les Etats-Unis ont finalisé leur dispositif avec la création de l'Adocacy Center", avant de se déclarer prêt "à renseigner sur le plan technique ou à fournir des données économiques aux entreprises n'ayant pas la capacité de se les procurer directement."

Pour ce qui est de la société civile, les forces de l'ordre et services de renseignement américains ont aussi mené un intense travail de lobbying auprès des 41 pays membres du Conseil de l'Europe pour que la surveillance de l'internet soit effectuée, a priori, sur toutes les télécommunications de leurs citoyens, et leurs correspondants, sous couvert de lutte contre la cybercriminalité.

Suite aux attentats du 11 septembre 2001, les USA ont aussi imposé aux compagnies aériennes de mettre à leur disposition les données personnelles de leurs passagers -quand bien même cela allait à l'encontre du droit européen-, et exigés l'adoption, dans le monde entier, de passeports biométriques. Entre autres échanges de données informatisées, grandement facilités depuis.

Conclusion

Echelon, Frenchelon et ses pairs ne sont pas prêts de disparaître, d'autant que la tendance est aujourd'hui à la banalisation des diverses formes de surveillance. La vidéosurveillance se fait « intelligente », les puces RFID commencent à être couplées aux modules de géolocalisation GPS, la traçabilité devient la norme, la vie privée un obstacle à la sécurité, « première des libertés ».

Ce que la technologie permet, la loi l'autorise. Ce qui, il y a quelques années, avant l'explosion de l'internet et de ses « nouvelles technologies », n'aurait pu passer, parce que la société civile aurait été scandalisée, et que les politiques auraient réagi, passe aujourd'hui comme une lettre à la Poste. Il suffit d'intaller tel ou tel logiciel, et de « cliquer là ».

La nouvelle loi Informatique et Libertés va ainsi à l'encontre de ce pour quoi elle avait initialement été adoptée. En 1978, elle visait à proscrire les dérives connue par la France, en matière de fichage de la population, sous l'occupation. Sa révision, en 2004, a libéralisé la création de fichiers administratifs et policiers, ôtant à la CNIL tout pouvoir de blocage de telles interconnexions.

Si l'espionnage (militaire, politique, économique) fait traditionnellement fi de la loi, le fait que la surveillance administrative et policière soit légalisée, et que leurs technologies fassent partie des secteurs de l'industrie « high tech » les plus en vue, et rémunérateurs, fait pour le moins le lit de « Big Brother ». A ceci prêt qu'il n'y a pas « un » Big Brother, mais qu'ils sont légions.

La question est moins celle des seuls programmes Echelon et Frenchelon -si illégaux, onéreux et potentiellement liberticides soient-ils- que celle de cette société de l'information qui, sous couvert d'administration et de gouvernance électronique, d'optimisation du marché par la traçabilité et de lutte contre l' « insécurité », tend de plus en plus vers une société de surveillance.

REF :
http://vie-privee.org
http://jean-marc.manach.net/
http://bigbrotherawards.eu.org
http://www.bugbrother.com/echelon/
http://groups-beta.google.com/group/guerrelec/