(Source : l'Actualité – Merci à Clara)

(Photo: Pixabay)

Parlons de votre droit à la vie privée, qui s'est effrité petit à petit au fil des années.

Vos grands-parents pouvaient décider de partir au chalet pour la fin de semaine et personne ne le savait. Vous, c'est différent. Votre cellulaire indique constamment votre position à votre service téléphonique. L'application GPS que vous utilisez pour connaître le bon chemin vous suit également à la trace. Le petit café où vous vous arrêtez en cours de route offre le Wi-Fi gratuitement. Pendant que vous grignotez une pâtisserie, l'identifiant unique de votre téléphone et les sites Web que vous consultez sont gardés en mémoire. À la petite épicerie du village où vos grands-parents auraient payé comptant, vous avez sorti votre carte de crédit: l'opération a été enregistrée et sera conservée. Sur Facebook et Instagram, vous publiez ces photos de magnifiques paysages enneigés, ajoutant une pièce de plus à votre autobiographie numérique.

Si quelqu'un obtient ces empreintes électroniques que vous disséminez lors de vos pérégrinations, il peut alors reconstituer votre existence. Vos déplacements, vos achats, vos

loisirs, vos interactions sociales. **Non seulement votre passé peut être fouillé, mais votre avenir proche peut être prédit.**

«Et alors?» pensez-vous sans doute à ce moment. «Qu'est-ce que ça change si on sait que je suis allé au chalet? Je n'ai rien à cacher.»

C'est vrai, le chalet est anodin. **Mais une clinique d'avortement? Le bureau d'un psychiatre? Une rencontre pour alcooliques anonymes? Une célébration religieuse? Et je ne parle même pas de vos achats. Un jouet sexuel? Une revue politique d'extrême droite ou d'extrême gauche?**

«Bah! Qui s'intéresse à ma vie? Je ne suis personne…»

Peut-être bien. **Pour l'instant.** Mais beaucoup de choses ont changé ces dernières années. Auparavant, pour surveiller un suspect, il fallait une équipe de plusieurs personnes. Aujourd'hui, une seule derrière un écran peut en surveiller des milliers, voire des millions. **Les autorités recueillent de gigantesques quantités de données, et les trient ensuite à la recherche de quelque chose de louche. Si vous êtes au mauvais endroit au mauvais moment, vos données peuvent faire partie du lot, être un jour ou l'autre utilisées, que vous soyez un suspect ou non, que vous le vouliez ou pas, et être conservées pendant une période indéterminée.**

De nombreux indices glanés par les médias, recueillis par des fonctionnaires, déposés en preuve devant les tribunaux ou rendus publics par des lanceurs d'alerte portent à croire qu'une entité ayant de tels pouvoirs existe: **notre gouvernement.** Son objectif, louable, est de surveiller de potentielles menaces à notre sécurité et de nous en préserver. Mais peut-être avons-nous laissé s'emballer cette machine censée nous protéger.

Notre droit à la vie privée s'est dissous dans un océan de données ces dernières années et certains événements semblent tirés d'un film d'espionnage. Pourtant, tout est vrai. Toutes mes sources sont en hyperliens. Pour faciliter la compréhension, je vous présente tous les faits en ordre chronologique.

Comme le disait l'ancien chef du Centre de la sécurité des télécommunications du Canada, John Adams, lors d'une entrevue exclusive accordée à la CBC en octobre 2013: «Si vous êtes sur Internet, c'est littéralement comme si vous étiez sur la première page du *Globe and Mail*.» L'ancien militaire était aux commandes de cette agence de renseignements, aux activités secrètes, de 2005 à 2011. En mai 2014, devant le caucus des sénateurs libéraux, il y

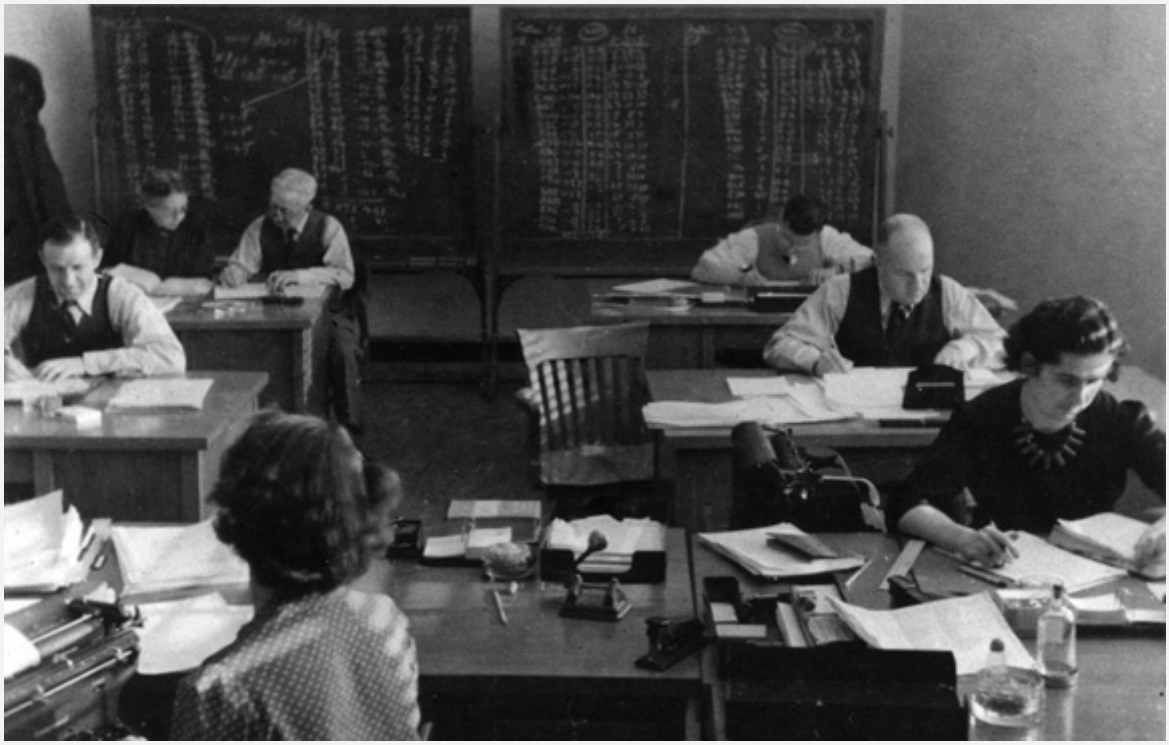
est allé d'une autre déclaration, cette fois à propos des internautes canadiens: «**La moitié [d'entre eux] est stupide et l'autre moitié est stupide [aussi]. […] Nous mettons davantage de choses sur Facebook que n'importe quel autre pays dans le monde. Nous ne sommes pas très intelligents, nous avons beaucoup de chemin à faire.**» Plutôt tranchant, pour celui qui était à la tête de l'une des plus importantes machines de surveillance du pays.

Au Canada, il existe deux agences fédérales spécialisées dans le renseignement: le Service canadien du renseignement de sécurité (SCRS) et le Centre de sécurité des télécommunications (CST). Le SCRS recueille et analyse des informations au Canada et à l'étranger pour déceler de potentielles menaces à la sécurité nationale. De son côté, le CST se spécialise dans la surveillance des télécommunications à l'étranger et dans la protection de l'infrastructure électronique de l'État. À elles deux, ces agences emploient 5 500 personnes et disposent d'un budget cumulé de 1,2 milliard de dollars pour 2016-2017.

Commentaire :

Surveiller et contrôler plutôt que nourrir et soigner…

Leur histoire remonte à la Deuxième Guerre mondiale. Les Forces canadiennes interceptaient des signaux électroniques cryptés en provenance d'armées étrangères. Des civils enrôlés au sein de la Sous-section de l'examen avaient pour mission de les déchiffrer. Après la guerre, en août 1946, la Direction des télécommunications du Conseil national de recherches est mise sur pied, et les 179 personnes qui tentaient de décoder les messages ennemis y sont intégrées. La création de ce nouveau service se fait grâce à un décret adopté en secret. Dès leurs débuts, les organismes de surveillance du Canada baignent dans une aura de mystère. L'organisme d'État travaillera dans l'ombre pendant trois décennies, avant d'être révélé au public par un documentaire de la CBC, en 1974. L'année d'après, il changera de nom pour devenir le Centre de sécurité des télécommunications.



La Sous-section de l'examen était une équipe civile qui avait pour mission de déchiffrer les signaux électroniques ennemis pendant la Deuxième guerre mondiale. (Photo: Centre de la sécurité des télécommunications)

En parallèle, pendant la guerre froide, la Gendarmerie royale du Canada est responsable de la collecte de renseignements liés à la sécurité nationale. Lors de la crise d'Octobre, en 1970, le gouvernement fédéral demande à la GRC d'accumuler des informations sur les militants souverainistes. Les policiers mettent en œuvre «une vaste campagne de collecte de renseignements, d'infiltration, de harcèlement et de perturbation visant la quasi-totalité des manifestations du sentiment nationaliste au Québec». Une multitude d'actes illégaux sont commis par les agents, dont notamment l'entrée par effraction dans les locaux du Parti québécois et le vol de la liste de ses membres.

Plusieurs reportages révéleront au public les agissements des policiers. En 1977, la pression est trop forte: le gouvernement de Pierre Elliott Trudeau institue une commission d'enquête sur les activités de la Gendarmerie royale du Canada. **On y apprend que les policiers mènent depuis des années des activités de surveillance qui n'ont jamais été autorisées par la loi, comme l'ouverture du courrier, par exemple.**

Commentaire :

À ajouter à la série du « *plus ça change, plus c'est pareil… sauf que c'est pire*« .

On recommande de retirer à la GRC la responsabilité du renseignement de sécurité. Selon la commission, l'équilibre entre la collecte de renseignements de sécurité et le respect des droits et libertés sera problématique tant que ce mandat restera entre les mains de policiers. En 1984, le Parlement décide finalement de voter une loi pour créer une agence civile spécialisée: le Service canadien du renseignement de sécurité (SCRS).

À la fin des années 1980, le Service canadien du renseignement de sécurité et le Centre de sécurité des télécommunications sont donc en place. Mais deux événements changent radicalement la nature et l'ampleur des moyens à la disposition des agences: **l'essor d'Internet et les attentats du 11 septembre 2001.**

Commentaire :

Tout aurait été soigneusement planifié que ça n'aurait pas pu être mieux fait. Mais ce serait là du complotisme, bien entendu.

Dans les années 1990, les communications numériques envahissent rapidement la vie quotidienne. Pour les agences de surveillance, c'est à la fois une manne extraordinaire et un défi de tous les instants. D'une part, la technologie évolue sans arrêt et devient de plus en plus complexe, et d'autre part, les lois régissant les pouvoirs d'enquête ont été écrites avant ces bouleversements technologiques, laissant les agences dans des impasses ou des flous juridiques.

Puis, survient l'écrasement de deux avions contre les tours du World Trade Center, à New York, le 11 septembre 2001. La Loi antiterroriste est rapidement déposée à la Chambre des communes et entre en vigueur dès le 18 décembre de la même année. Les élus, craignant d'autres attaques, dotent les agences de nouveaux pouvoirs et de nouveaux moyens. Le budget du SCRS a plus que triplé depuis les années 2000. Les effectifs du Centre de sécurité des télécommunications ont quant à eux doublé depuis la mise en place de la Loi.

Le 11 septembre 2001, deux avions percutent les tours jumelles du World Trade Center, à New York. (Photo: Associated Press / Gene Boyars)

Auparavant, le CST était uniquement autorisé à saisir des échanges électroniques à l'extérieur du pays. La Loi antiterroriste lui permet désormais de surveiller les communications en partance ou à destination du Canada. Le Centre n'a pas le droit de surveiller des citoyens canadiens, mais le changement législatif rend cette option possible si des échanges ont lieu avec une entité étrangère. Le CST n'avait pas le droit non plus d'intercepter des communications privées. La nouvelle loi lui accorde aussi ce pouvoir, à condition d'obtenir l'autorisation spéciale du ministre de la Défense. Tous ces changements sont majeurs. D'ordinaire, les autorités doivent obtenir un mandat d'un juge, qui s'assure de façon indépendante que les enjeux de sécurité justifient un tel empiètement sur la vie privée des personnes. Mais le CST, lui, n'a pas à se conformer à ce protocole. La décision revient au ministre, qui peut déclencher l'interception de milliers de communications en une seule autorisation. Selon un reportage diffusé par Radio-Canada en 2013, le ministre en avait signé

48 depuis la nouvelle loi.

En décembre 2005, le *New York Times* révèle que l'ancien président George W. Bush a secrètement autorisé l'espionnage de centaines, voire de milliers de citoyens aux États-Unis, et ce, sans aucun mandat, après les attentats du 11 septembre 2001. La même chose s'est-elle produite avec son équivalent canadien, le Centre de sécurité des télécommunications? Le commissaire du CST, l'ancien juge en chef de la Cour suprême du Canada Antonio Lamer, veut en avoir le cœur net. Son rôle est de s'assurer que l'agence d'espionnage respecte les lois, notamment la Charte canadienne des droits et libertés. Dans des documents obtenus par La Presse Canadienne en 2006, on apprend qu'une enquête interne de deux mois a été menée. **Mais les documents sont hautement confidentiels et de nombreuses parties ont été censurées.** Les conclusions du commissaire devaient être déposées devant le Parlement, dans son rapport annuel. Finalement, le document en question apporte bien peu de réponses. Aucune conduite illicite de la part du Centre n'a eu lieu, conclut le rapport, sans donner de détails.

L'année suivante, un nouveau commissaire entre en fonction, Charles D. Gonthier, lui aussi ancien juge à la retraite. Son rapport donne un aperçu beaucoup plus clair des opérations de surveillance du CST. En vertu de la loi, il est strictement illégal pour le Centre d'espionner expressément des citoyens canadiens, mais «lorsqu'il recueille des renseignements étrangers, le CST peut incidemment acquérir des renseignements personnels sur des Canadiens». Le Centre peut conserver ces renseignements s'il «les juge indispensables à la compréhension des renseignements étrangers». De plus, il peut divulguer ces informations, par exemple à la GRC, si un mandat est obtenu. Le CST peut aussi aider d'autres agences fédérales à collecter des renseignements, y compris sur des Canadiens, si un mandat a été obtenu.

À la fin des années 2000, la capacité de surveillance de masse du CST et du SCRS sont encore peu connus. Le rôle du CST, par exemple, est **d'«acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information». Mais qu'est-ce que cela signifie concrètement? Les citoyens et les élus n'ont pas la moindre idée de l'ampleur des opérations qui sont menées.** En vertu de la loi, ces agences ne rendent des comptes qu'au ministre de la Défense, qui est lui-même tenu au secret.

Survient alors le 9 juin 2013: le lanceur d'alerte Edward Snowden entre en scène et lève le voile sur les opérations les plus secrètes du gouvernement…

Le 9 juin 2013, Edward Snowden sort de l'ombre. L'Américain de 29 ans a travaillé pendant quatre ans pour la National Security Agency (NSA), l'agence d'espionnage des États-Unis. Le lanceur d'alerte donne aux journalistes des milliers de documents ultrasecrets qui mettent au jour un système de surveillance de masse. Comme la NSA collabore très souvent avec les agences canadiennes, certains documents émanent directement de ces dernières. Pendant des mois, des journalistes s'affaireront à trier et à tenter de confirmer l'authenticité de tous les documents donnés par Snowden. Les Canadiens ne le savent pas encore, mais des révélations explosives feront bientôt les manchettes…

Entre-temps, les remises en question des services de renseignements s'enchaînent. En juin 2013, le commissaire sortant du Centre de sécurité des télécommunications, Robert Décary, présente son dernier rapport sur les activités de l'agence d'espionnage. L'ancien membre de la Cour fédérale d'appel souligne que certaines données sur les opérations passées du CST, qui permettent normalement de s'assurer que les cibles du Centre sont «bel et bien étrangères et situées à l'extérieur du Canada», sont manquantes. «L'absence d'information a limité ma capacité à évaluer la légalité des activités du Centre à cet égard», écrit le commissaire. Plus loin dans son rapport, un autre passage montre les limites de sa capacité d'examiner les actions de l'agence d'espionnage: «Un petit nombre de dossiers suggéraient la possibilité que des Canadiens aient été visés par certaines activités, ce qui est contraire à la loi. Certains dossiers du Centre relatifs à ces activités n'étaient pas clairs ou étaient incomplets. **Après un examen minutieux et approfondi, je n'ai pas pu parvenir à une conclusion définitive sur la conformité ou non à la loi.**»

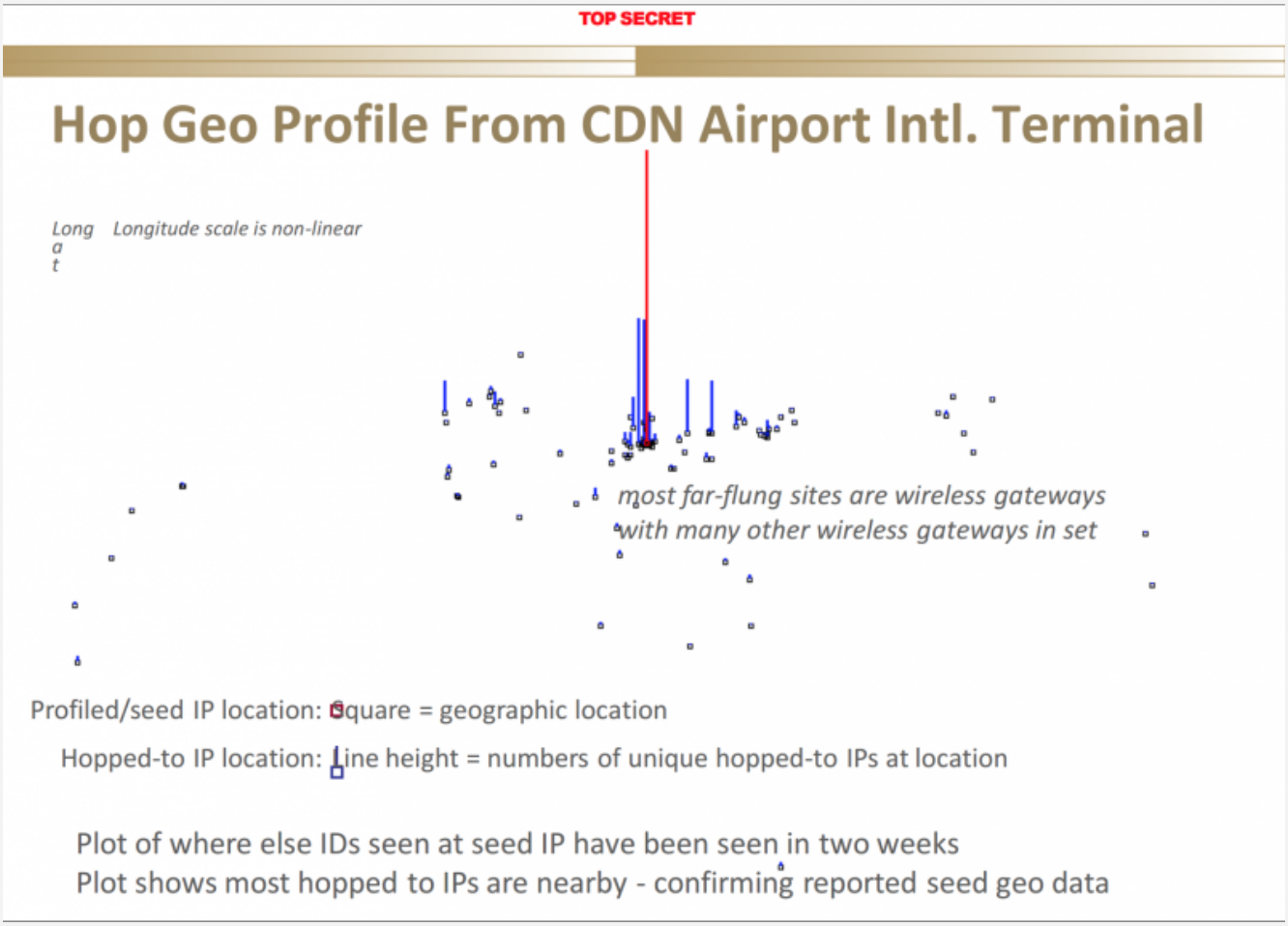
Les mois qui suivent ne sont pas de tout repos pour les agences de renseignements, qui continuent de se retrouver à la une des journaux. En octobre 2013, c'est l'ancien chef du CST lui-même, John Adams, qui soutient lors d'une entrevue à la CBC qu'il faut une plus grande supervision des activités de l'agence d'espionnage.

Un mois plus tard, en novembre 2013, le juge de la Cour fédérale Richard Mosley rend une décision dans laquelle il conclut que le SCRS et le CST ont délibérément caché des informations à la Cour. L'affaire remonte à 2009. Les agences d'espionnage demandent un mandat spécial pour surveiller deux citoyens canadiens à l'extérieur du pays. Les autorisations sont données par le juge Mosley, à condition que les opérations soient menées par des fonctionnaires canadiens, à partir du Canada. Cinq ans plus tard, alors que le juge fait un suivi de l'affaire, il se rend compte que les agences ont en fait demandé à des autorités

étrangères de surveiller les citoyens canadiens à leur place. «Compte tenu que, au cours des 10 dernières années, le partage de renseignements avec des agences étrangères a souvent mal tourné […], il ne fait aucun doute que les agences canadiennes sont conscientes de ces dangers», indique le juge Mosley dans sa décision, faisant écho à l'affaire Maher Arar. Cet ingénieur canadien a été expulsé vers la Syrie en 2002, alors qu'il revenait de vacances en Tunisie en passant par New York, à cause de fausses informations provenant de la GRC, qui le soupçonnait d'être un activiste terroriste. Emprisonné et torturé dans son pays d'origine, il a finalement été blanchi quatre ans plus tard, après une enquête publique qui a coûté 15 millions de dollars.

Puis, le 28 janvier 2014, c'est au tour de la Commissaire à la protection de la vie privée du Canada de demander davantage de transparence au Centre de sécurité des télécommunications, dans un rapport spécial au Parlement. «**La manière dont [les activités de renseignements] sont menées peut ouvrir la voie à une collecte à grande échelle, écrit Chantal Bernier. L'information […] comme celle que l'on retrouve sur les sites de réseautage social, est balayée électroniquement et a le potentiel de devenir la principale source de renseignement. […] Le potentiel d'atteinte à la vie privée dans ce nouveau contexte est tel qu'il exige une protection de la vie privée proportionnelle.**»

Ironie du sort, deux jours seulement après l'appel de la Commissaire à davantage de transparence, les journalistes de la CBC sont prêts à rendre publiques les révélations d'Edward Snowden. Dans un des documents donnés par le lanceur d'alerte et daté du 10 mai 2012, une révélation explosive: le Centre de sécurité des télécommunications a recueilli des métadonnées sur toutes les personnes qui s'étaient connectées au réseau Wi-Fi d'un aéroport canadien, pendant deux semaines. Dans le même document, on apprend aussi que le Centre a balayé une «ville de taille modeste». Ses employés se sont attardés à deux réseaux sans fil en particulier, auxquels 300 000 appareils différents se sont connectés sur une période de deux semaines. Il n'est pas indiqué dans le document si cette autre opération s'est déroulée au Canada, mais selon la CBC, ce serait le cas. Le CST s'intéressait aussi à d'autres aéroports, en plus d'hôtels, de cafés et de bibliothèques publiques.



Un des documents secrets du Centre de sécurité des télécommunications du Canada qui a été révélé au public par Edward Snowden. (Source: Snowden Surveillance Archive / Canadian Journalists for Free Expression)

Après ces révélations, le chef du CST doit s'expliquer devant le Comité sénatorial permanent de la Sécurité nationale et de la défense, le 3 février 2014. On y apprend que les métadonnées avaient été recueillies à l'aéroport international Pearson, à Toronto, le plus fréquenté du pays. «L'opération faisait partie de notre collecte de données habituelle à l'échelle mondiale», indique John Forster, avant d'ajouter que «les terroristes ou les auteurs de prises d'otages accèdent souvent à Internet dans les lieux publics, comme un aéroport ou un café, parce qu'ils essaient de se cacher au milieu de la foule». Ses équipes essayaient de mettre au point un logiciel pour identifier une cible dans la nuée des millions d'échanges et de connexions qui ont lieu en même temps sur Internet. «Je sais que ce modèle a été utilisé au moins deux fois au cours des 12 derniers mois pour trouver des cibles étrangères légitimes», ajoute John Forster pour défendre son service.

Lors de cette audience sénatoriale, on découvre aussi que deux directives ministérielles ont été signées, l'une en 2005, par le libéral Bill Graham, et l'autre en 2011, par le conservateur Peter MacKay. Ces deux directives autorisaient le CST à conserver des métadonnées, comme celles de l'aéroport Pearson, pendant une durée déterminée. «S'agit-il d'une directive secrète?» a demandé le sénateur Hugh Segal. «Oui», a répondu John Foster. Impossible donc de savoir si les données de l'aéroport Pearson ont été détruites ou si elles sont toujours entre les mains de l'agence.

Les enjeux de sécurité percutent de plein fouet le droit à la vie privée des personnes. Deux événements jettent de l'huile sur le feu: l'attentat de Saint-Jean-sur-Richelieu et la fusillade au parlement, en octobre 2014. Encore une fois, la question se pose: où se trouve la limite entre le respect de la vie privée et la surveillance de l'État au nom de la sécurité nationale?

Le 27 janvier 2015, les journalistes qui ont étudié les documents donnés par Edward Snowden publient une nouvelle bombe: une opération nommée Levitation permet au Centre de sécurité des télécommunications de surveiller des centaines de millions de téléchargements sur des sites d'échanges gratuits, tout autour de la planète. Selon le document, datant de 2012, le CST épie de 10 à 15 millions de téléchargements par jour. Une dizaine d'entre eux sont dits «intéressants» au quotidien. Le filet du CST est tellement large qu'une des pages du document est intitulée «Filtrer les épisodes de *Glee*», série télévisée populaire très téléchargée. Selon la CBC, ce serait une note d'humour de la part des employés du CST.

Lorsque l'agence détecte un téléchargement suspect, par exemple un manuel pour fabriquer des explosifs, elle est capable de reconnaître l'adresse IP de l'ordinateur utilisé. À partir de cet identifiant, elle peut alors repérer toutes les activités faites sur cet appareil cinq heures avant et après le téléchargement. Si la personne s'est connectée à son profil Facebook pendant cette période, le Centre est ainsi capable de l'identifier. Deux adresses IP canadiennes, localisées à Montréal, se trouvaient dans le document non censuré, d'après la CBC. Selon la fiche descriptive du système Levitation, le logiciel a permis de découvrir la vidéo d'un otage allemand ainsi que des documents stratégiques d'al-Qaïda au Maghreb islamique. On ne sait pas si ce sont là ses seuls succès.

Dès le lendemain de la diffusion du reportage sur le sujet par la CBC, les réactions fusent de toutes parts. D'un côté, le ministre associé à la Défense nationale, le conservateur Julian Fantino, pour justifier les opérations, déclare que «notre gouvernement ne restera pas

immobile pendant que les terroristes utilisent des sites Web pour attirer, radicaliser et entraîner des individus qui menacent nos valeurs et notre liberté». Le chef du Parti libéral et futur premier ministre, Justin Trudeau, rétorque qu'il est «temps de parler d'une supervision adéquate pour s'assurer que le gouvernement agit de façon responsable».

La députée néo-démocrate de Portneuf–Jacques-Cartier, Élaine Michaud, renchérit lors de la période des questions: «**Le gouvernement veille-t-il à ce que les activités personnelles des Canadiens ne soient pas surveillées, pour ne pas dire espionnées? Comment s'assure-t-il de protéger la sécurité des Canadiens, tout en préservant leur vie privée?**»

Commentaire :

Vie privée. Quelle vie privée?

Julian Fantino se contente de répondre que le commissaire du Centre de sécurité des télécommunications «a confirmé qu'elles étaient conformes à la loi».

Pour rappel, le commissaire du CST doit s'assurer que **le Centre agit en toute légalité**. C'est généralement un juge à la retraite qui occupe ce poste à temps partiel. Il dispose d'une équipe de 11 personnes pour surveiller les activités des 2 200 employés du CST. Depuis sa création, en 1996, le Bureau du commissaire du CST n'a jamais constaté la moindre activité illégale, sauf une fois, en 2016, et c'était parce que… le CST l'avait prévenu.

Les révélations des journalistes et l'indignation des partis politiques d'opposition n'empêcheront pas le gouvernement conservateur de Stephen Harper de déposer le projet de loi C-51 deux jours après les révélations, le 30 janvier 2015, pour… donner encore plus de pouvoirs aux agences. Pour l'opposition, ce texte de loi va trop loin. «Comment peut-on empêcher que ce projet de loi soit utilisé pour espionner les ennemis politiques du gouvernement?» s'inquiète le chef du NPD, Thomas Mulcair.

Commentaire :

Voir aussi :
Canada : le projet de loi C-51 pourrait criminaliser la dissidence, rien de moins

Canada : plus de pouvoirs de surveillance aux agences de renseignement

Le Commissaire à la protection de la vie privée du Canada, Daniel Therrien, décide alors de prendre position. Dans une lettre ouverte publiée dans des quotidiens du pays, il soutient que la nouvelle loi fera en sorte que «**tous les citoyens seront pris dans cette toile, pas**

seulement ceux soupçonnés de terrorisme». En vertu de la loi, 17 nouveaux organismes pourront échanger et recevoir des informations du SCRS. Or, 14 d'entre eux ne font l'objet d'aucune surveillance indépendante. «Le terrorisme représente une menace croissante. Des mesures s'imposent en matière de sécurité nationale. Mais à quel prix? […] **Ces nouveaux pouvoirs sont démesurés et les mesures de protection de la vie privée proposées sont nettement insuffisantes.**»

Le 25 mars 2015, la nouvelle chef du CST, Greta Bossenmaier, témoigne devant le Comité permanent de la défense nationale. La députée du NPD, Élaine Michaud, lui rappelle les opérations secrètes d'aspiration de données de l'aéroport Pearson et de surveillance des téléchargements, avant de lui poser sa question: «Pouvez-vous confirmer cela ou nous donner plus de précisions sur cette nouvelle vocation plus offensive que semble prendre le CST?» Réponse de la patronne du CST: «J'espère que vous comprenez qu'il m'est impossible de me prononcer sur la divulgation non autorisée d'informations classifiées.» La députée tentera à plusieurs reprises de pousser Greta Bossenmaier à répondre à ses questions. Sans succès. Elle baissera finalement les bras tout en concluant: «Il est essentiel de disposer d'un comité parlementaire de surveillance qui soit habilité en matière de sécurité de façon à pouvoir analyser ce qui se passe. À l'heure actuelle, la reddition de comptes est strictement impossible à l'endroit des parlementaires. Ils ne peuvent pas non plus obtenir de réponses à des questions pourtant légitimes.»

Alors que le projet de loi C-51 poursuit son chemin à la Chambre des communes, Michael Doucet, directeur général du Comité de surveillance des activités de renseignement de sécurité (CSARS), s'inquiète lui aussi des possibles conséquences. Son comité a pour mandat de s'assurer que le Service canadien du renseignement respecte les droits et libertés des citoyens. «Le projet de loi C-51 aura un impact considérable, non seulement sur l'efficacité même du CSARS, mais sur la reddition de comptes en matière d'activités de renseignement de sécurité au Canada», dit-il dans son discours d'ouverture au comité sénatorial permanent de la sécurité nationale et de la défense, le 23 avril 2015. «L'adoption du projet de loi C-51 placerait le CSARS dans une position délicate où sa capacité de s'acquitter efficacement de ses fonctions de surveillance pourrait être compromise.»

Mais tous les avertissements venant des élus et des fonctionnaires ne changeront rien: le projet de loi C-51 est adopté sans amendement à la Chambre des communes le 6 mai 2015, grâce à la majorité conservatrice et à l'appui libéral, dont notamment celui de Justin Trudeau,

futur premier ministre.

Le SCRS est alors doté de nouveaux pouvoirs, dont celui d'«atténuation de la menace». C'est un tournant historique. Le Service se contentait jusqu'à présent de recueillir de l'information, de l'analyser et de guider le gouvernement dans ses décisions. Désormais, l'agence d'espionnage peut perturber des transactions financières, des voyages ou des communications au pays ou à l'étranger, s'il existe «des motifs raisonnables de croire qu'une activité donnée constitue une menace envers la sécurité du Canada». De plus, la Loi sur la communication d'information ayant trait à la sécurité du Canada ayant aussi été créée, le SCRS n'a plus besoin du mandat d'un juge pour obtenir, par exemple, des informations provenant de l'Agence du revenu du Canada.

En juillet 2015, le *National Post* publie un document apparemment secret du Conseil du Trésor, divulgué par le groupe Anonymous. Alors que le gouvernement n'avait admis l'existence que de trois stations d'opération étrangères du Service canadien du renseignement de sécurité (à Washington, Londres et Paris), le document stipule qu'il y en aurait 25, «dont la plupart se trouvent dans des pays en voie de développement et/ou dans des environnements instables». Quelque 70 employés seraient chargés d'y traiter environ 22 500 messages par an. Il semblerait de plus qu'elles soient en fonction depuis au moins 30 ans, puisqu'il est précisé dans le document que ces stations n'ont pas été rénovées «depuis que les activités de collecte étrangères du Service ont commencé, au milieu des années 1980». Le gouvernement n'a pas confirmé l'authenticité de ce document.

Le 19 octobre 2015, Justin Trudeau et les libéraux prennent les commandes de la Chambre des communes. Une de leurs promesses: reprendre le pouvoir sur les agences d'espionnage. Mais le début de leur règne commence avec de nouveaux déboires…

En 2016, les révélations continuent d'accaparer les agences d'espionnage. En janvier, pour la première fois de son histoire, le commissaire du Centre de sécurité des télécommunications écrit au ministre de la Défense et au procureur général du Canada «pour les informer qu'il avait découvert que le CST ne se conformait pas à la Loi sur la défense nationale et à la Loi sur la protection des renseignements personnels». Le CST échange régulièrement des informations avec des partenaires étrangers. Lorsque ces données concernent des Canadiens, le Centre doit les anonymiser, ce qui n'avait pas été fait correctement, indique Jean-Pierre Plouffe, selon qui «le CST n'avait toutefois pas agi avec une diligence raisonnable».

La polémique se poursuit en février, lorsque le commissaire Jean-Pierre Plouffe témoigne devant le Comité sénatorial permanent de la Sécurité nationale et de la défense. On y apprend que le manquement a duré pendant des années. Il a été découvert en novembre 2013, et la procédure a été arrêtée en 2014, bien que le public n'en ait été prévenu qu'en 2016. «Parle-t-on de centaines de milliers [de Canadiens touchés]?», demande le sénateur Claude Carignan. «Il est impossible de déterminer quoi que ce soit», lui répond le commissaire.

En juin, c'est le *Globe and Mail* qui en apprend davantage, grâce à des documents confidentiels déposés devant les tribunaux. Le partage d'informations non anonymisées sur des Canadiens remonterait jusqu'en 2005 et comporterait des listes d'appels téléphoniques et d'échanges par Internet. Selon le document, pour les courriels, les adresses étaient anonymisées, mais pas les adresses IP. Et le CST lui-même ne sait pas quelle est l'ampleur de cette erreur qui a duré probablement pendant près d'une décennie. Le contenu des messages, *a priori,* n'aurait pas été collecté.

Puis, en novembre 2016, c'est de nouveau au tour du SCRS de se faire taper sur les doigts. Le juge de la Cour fédérale Simon Noël rend une décision sans équivoque: «Le SCRS a manqué, une fois encore, à son obligation de franchise envers la Cour.» Depuis 2006, le SCRS conservait des métadonnées, obtenues auprès de fournisseurs de service, «même si le contenu auquel elles sont associées n'était pas considéré comme lié à une menace». De nombreuses parties du jugement étant confidentielles, il est difficile de savoir de quoi il s'agit exactement. Toutefois, ces données étaient traitées par un puissant logiciel nommé Operational Data Analysis Centre, qui permettait de donner «un portrait précis et intime de la vie et de l'environnement des personnes sur lesquelles le SCRS enquête. Le programme permet d'établir des liens entre diverses sources et d'énormes quantités de données, ce qu'aucun humain n'arriverait à faire.» Sauf que la Cour n'a jamais autorisé le Service à conserver les données en question, et donc, que le programme était illégal dès ses débuts, il y a 10 ans. «Il est peut-être temps que les Canadiens relancent le débat sur le mandat et les fonctions de son service de renseignement national», ajoute le juge Noël dans sa décision.

Justement, les libéraux, bien qu'ils aient voté pour le projet de loi C-51, ont aussi promis lors de la dernière campagne électorale qu'ils «ramèneront l'équilibre entre notre sécurité collective et nos droits et libertés». Une consultation est d'ailleurs en cours sur le sujet depuis le 8 septembre. Les Canadiens ont jusqu'au 15 décembre pour y participer.

Nous surveillerons de plus près notre appareil de sécurité nationale.

À l'heure actuelle, le Parlement n'assure aucune surveillance de nos organismes de sécurité nationale, ce qui fait du Canada le seul pays du Groupe des cinq où les élus n'exercent aucun contrôle sur les services de sécurité. La population s'en trouve mal informée et mal représentée dans des dossiers fondamentaux.

Nous créerons un comité multipartite qui devra surveiller les opérations de tous les ministères et organismes fédéraux chargés de la sécurité nationale.

Extrait de la plateforme électorale de Justin Trudeau lors de l'élection générale de 2015. (Source: Site Web du Parti libéral du Canada)

Mais le débat semble aujourd'hui dépasser les agences de surveillance fédérales. **Les services policiers, eux aussi, utilisent de plus en plus des techniques qui menacent la vie privée de milliers de personnes qui ne sont suspectées d'aucun crime.**

En avril dernier, on apprenait que la Gendarmerie royale du Canada utilisait secrètement depuis 2005 un appareil pour surveiller tous les échanges téléphoniques ayant lieu dans une zone donnée, lors de certaines de ses enquêtes. Appelé Stingray ou IMSI Catchers, ce dispositif de la taille d'une mallette relève toutes les communications, sans discrimination, par exemple dans un quadrilatère d'appartements. Que vous soyez le suspect ou non, si vous êtes au mauvais endroit au mauvais moment, vos communications peuvent donc être épiées, et vous ne le saurez jamais. Par ailleurs, au Canada, tous les appareils utilisant les ondes radio doivent être approuvés par une agence fédérale, et ces appareils ne l'ont jamais été.

Mais ce n'est pas tout. Dans des documents déposés devant les tribunaux, la GRC a aussi été forcée de révéler cette année qu'elle disposait de la clé globale de cryptage des téléphones BlackBerry. Sur ces appareils, les messages sont tous cryptés lorsqu'ils transitent entre deux interlocuteurs. Si quelqu'un intercepte ces messages, il est en théorie impossible pour lui d'en connaître le contenu. Sauf qu'il existe une clé universelle pour les déchiffrer et que les policiers fédéraux la possédaient depuis au moins 2010. Lors d'une enquête menée à Montréal à pareille date, la GRC a intercepté et déchiffré près d'un million de messages grâce à cette technique. Dans les documents déposés devant le juge, la Gendarmerie a indiqué que cette technologie équivalait à «**avoir les clés pour déverrouiller les portes des maisons de tous les utilisateurs, sans qu'ils le sachent**».

Les services de police municipaux semblent aussi avoir de plus en plus d'appétit pour de vastes quantités de données concernant les citoyens. En avril 2014, la police régionale de Peel, en banlieue de Toronto, enquête sur une série de braquages de bijouteries. Pour identifier les voleurs, les policiers réclament à Rogers et à Telus le relevé de «tous les téléphones activés, ayant transmis et reçu des données» de toutes les tours de réception cellulaire «à proximité de 21 adresses civiques», pendant la période des cambriolages. La quantité de données est énorme. En une seule requête, les policiers recevraient les informations téléphoniques, nominatives et bancaires de près de 43 000 personnes. La Cour supérieure de l'Ontario a jugé la demande excessive et l'a rejetée. Toutefois, dans la décision du juge John Sproat, on apprend que de telles demandes sont loin d'être exceptionnelles et que les policiers s'en servent régulièrement.

Selon le plus récent rapport du Commissaire à la protection de la vie privée du Canada, Daniel Therrien, «90 % des Canadiens ont l'impression de perdre le contrôle qu'ils exercent sur leurs renseignements personnels et s'attendent à être mieux protégés». Le Commissaire souligne que la Loi sur la protection des renseignements personnels a été promulguée en 1983 et la Loi sur la protection des renseignements personnels et les documents électroniques est entrée en vigueur en… 2001. Mark Zuckerberg avait alors 17 ans et Facebook n'existait pas.

La menace, il est vrai, est réelle. Le 7 mars 2016, devant le Comité sénatorial permanent de la sécurité nationale et de la défense, le directeur du Service canadien du renseignement de sécurité rappelait que 180 personnes ayant des liens avec le Canada mènent des activités terroristes à l'étranger. Selon Michel Coulombe, une centaine d'entre eux se trouveraient en

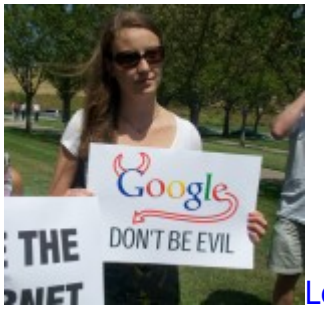
Irak et en Syrie. «Comme la participation des Canadiens à ces conflits nuit aux pays où ils se trouvent et les déstabilise, le Canada a l'obligation internationale d'empêcher les voyages à des fins terroristes.» Il y a aussi toute la question de ceux qui reviennent au pays — une soixantaine, selon le directeur — et qu'il faut surveiller. Sans compter les attaques informatiques, de plus en plus nombreuses et perfectionnées.

Mais comment surveiller ceux qui sont suspectés d'avoir commis des crimes sans enfreindre la vie privée des gens qui ne sont suspectés de rien? Comment garder un œil sur ceux qui *pourraient* poser une menace à la sécurité sans fouiller dans la vie de tout le monde? Quels sont les critères qui déterminent ce qu'est une menace? L'histoire regorge de trop nombreux exemples dramatiques où un gouvernement en savait tout d'un coup beaucoup trop sur les orientations politiques, l'origine ethnique ou la religion de ses citoyens.

Dans une démocratie, c'est aux citoyens de décider à quel point ils sont prêts à laisser l'État fouiller dans les aspects les plus intimes de leur vie. Mais les preuves des dernières années montrent combien les Canadiens ne connaissent pas les capacités des autorités publiques. Et c'est pourtant crucial, car le droit à la vie privée, c'est le droit d'être soi-même, en toute liberté.

À lire également :

Du droit à violer la vie privée des internautes au foyer



Le diable Google sort de sa boîte : qu'allons-nous faire?

L'ampleur insoupçonnée de ce que Facebook sait de vous uniquement grâce à vos « j'aime »


États-Unis : les banques observent les profils Facebook avant d'accorder un prêt