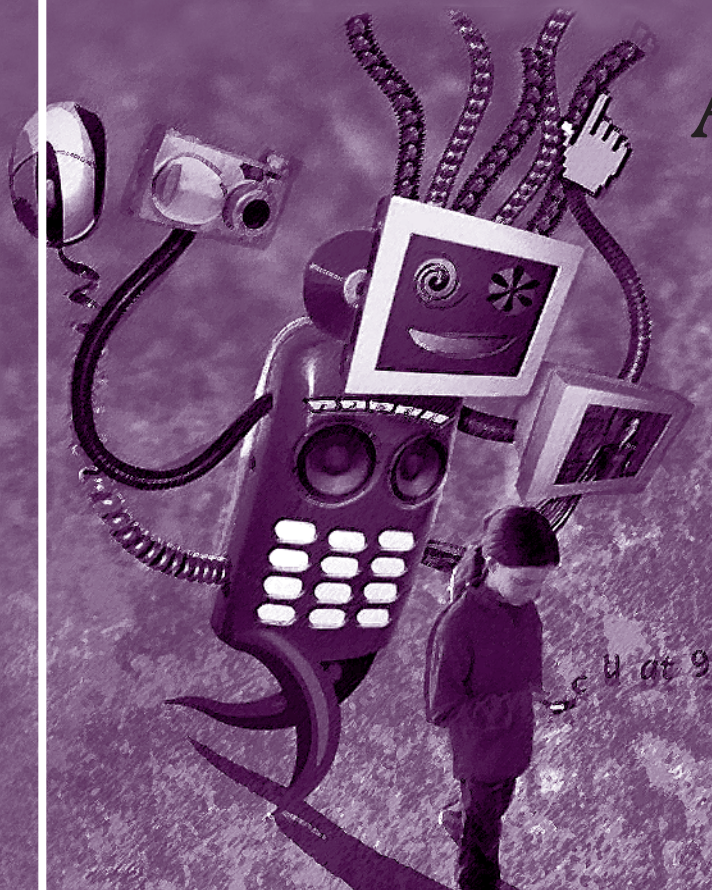


La surveillance de nos communications

Avons-nous
vraiment
rien à
craindre ?



La Fondation
Léo-Cormier



LIGUE DES DROITS ET LIBERTÉS

Novembre 2009

Une intrusion sans précédent dans la vie privée

Le gouvernement fédéral a présenté, en juin dernier, deux projets de loi, C-46 et C-47, qui donnent aux autorités de nouveaux pouvoirs de surveillance des communications des Canadien-nes.

Le gouvernement présente ces projets de loi comme une adaptation nécessaire aux nouvelles technologies des communications, des pouvoirs d'enquête traditionnels pour l'écoute téléphonique. À une époque où les nouvelles technologies de l'information et des communications envahissent notre vie quotidienne, des pans de plus en plus importants de notre vie sont numérisés. Ainsi, il n'y a pas de commune mesure entre l'information transmise lors d'une conversation téléphonique et celle qui circule électroniquement. De plus, contrairement à la conversation téléphonique, dont les paroles s'envolent, à moins d'avoir été enregistrées, les communications modernes laissent dans les mémoires des ordinateurs des traces qui peuvent être suivies longtemps après les faits.

Les milliers de faits et gestes qui constituent la vie de chacun pourraient devenir l'objet d'examens policiers : en premier lieu, les sites électroniques visités par chacun, le courrier électronique reçu ou envoyé, l'utilisation de la carte de crédit, les achats de toute nature (vêtements, livres, équipements divers), les sorties,



les déplacements à l'étranger mais aussi au pays (par les achats d'essence, etc.), ainsi que toutes les informations qui circulent dans un système informatique et, à ce titre, les transactions bancaires faites par Internet ou au guichet et les informations médicales. Et la liste pourrait évidemment s'allonger.

Il faut souligner le caractère très étendu des données soumises à ces nouveaux pouvoirs d'enquête. En effet, la définition de données informatiques dans les projets de loi comprend toute donnée qui est sous une forme qui permet le traitement par un ordinateur, ce qui représente en fait toute donnée numérisée. Les projets de loi couvrent donc également les objets et les biens, qui transmettent des informations sous forme numérique qui peuvent être reliées à un individu. Dans un monde d'objets dotés de GPS et de puces d'identification par radiofréquence (RFID), les possibilités de surveillance sont quasi illimitées.

Une entente internationale de surveillance des communications

La Convention sur la cybercriminalité est à l'origine de ces projets de loi. Cette Convention a été élaborée par le Conseil de l'Europe avec la participation active du Canada, des États-Unis, du Japon et de l'Afrique du Sud. Jusqu'à l'été 2001, les négociations sur la Convention semblaient vouées à l'impasse. Puis, les attentats du 11 septembre 2001 ont fourni le prétexte pour justifier une surveillance accrue des télécommunications. En effet, le texte définitif a été adopté en novembre 2001 et signé par le Canada en août 2002. En signant la Convention, les pays s'engagent à se doter de législations facilitant la surveillance électronique des communications.

En 2002, le gouvernement tient une consultation « quasi secrète » sur un projet intitulé Accès légal, par la suite renommé Accès licite. Les réponses des représentants du gouvernement aux questions que suscite le projet sont on ne peut plus vagues et la réaction des participants à la consultation est plutôt négative.

Ainsi, à l'automne 2005, la ministre de la Sécurité publique, Anne McLellan, soumettait le projet de loi C-74 – *Loi sur la modernisation des techniques d'enquête*. Toutefois, le projet de loi est mort au feuilleton lors du déclenchement des élections en 2006.

Le 18 juin 2009, le gouvernement Harper est revenu à la charge avec les projets de loi C-46 – *Loi sur les pouvoirs d'enquête au 21^e siècle* et C-47 – *Loi sur l'assistance au contrôle d'application des lois au 21^e siècle*.

« Si on a rien à se reprocher, on a rien à craindre »

C'est ce que pensait Mme Jenny Paton, résidente du comté Dorset en Angleterre et mère de trois enfants, jusqu'au jour où elle apprit que le registre de ses appels téléphoniques avait été épluché par les autorités de son conseil de comté et qu'elle avait fait l'objet d'une filature. Le crime dont on soupçonnait - à tort - Mme Paton? Avoir falsifié son adresse pour pouvoir inscrire ses enfants à l'école du comté!

Pour surveiller Mme Paton le conseil de comté s'est appuyé sur le *Regulation of Investigatory Powers Act (RIPA)*, la loi britannique d'accès licite. Suite à une plainte de Mme Paton, l'*Office of Surveillance Commissioners* qui surveille l'application de RIPA a statué que le conseil de comté n'avait pas agi incorrectement à l'égard de Mme Paton.

Des pouvoirs étendus

Les dispositions de C-46 et C-47 en bref :

- L'obligation pour les fournisseurs de services de communications de se doter des moyens de préserver les données de transmission, d'intercepter les communications et de préserver leur contenu afin de les rendre disponibles aux autorités. Cette obligation crée le dangereux précédent de coopter des personnes privées dans des enquêtes criminelles;
- L'obligation, pour les fournisseurs de services, de remettre les données sur leurs clients (nom, adresse, numéro de téléphone, adresse courriel, code d'identification de l'utilisateur – adresse IP) sans mandat judiciaire;
- La possibilité de saisir les données de transmission, c'est-à-dire les données relatives aux personnes et dispositifs avec lesquels une personne a communiqué, après avoir obtenu un mandat sur le simple *motif raisonnable de soupçonner*, lequel requiert un niveau de justification peu exigeant. Pourtant, la connaissance de l'ensemble des sites et des personnes avec lesquels une personne communique révèle des choses aussi privées que ses réseaux sociaux, ses champs d'intérêt, son orientation sexuelle... ;
- L'obligation, pour les fournisseurs de conserver les données - en attendant une éventuelle saisie - pendant 21 jours sur la base du *motif raisonnable de soupçonner* et sur simple demande d'un agent de la paix. Suite à la décision d'un juge, le fournisseur peut être obligé de conserver les données pour une période, renouvelable, de 90 jours;
- La saisie des données (contenu des transmissions) sur la base plus exigeante du *motif raisonnable de croire*. Cependant, contrairement à l'écoute téléphonique, l'agent n'aura pas à démontrer la nécessité d'avoir recours à des moyens plus intrusifs. La personne ne saura jamais que les données ont été saisies alors que dans le cas de l'écoute électronique la personne qui a fait l'objet de la surveillance doit en être informée 90 jours après la fin de celle-ci;
- La possibilité d'installer, sur des choses portées ou transportées par une personne physique, un dispositif de localisation, sur la base du *motif raisonnable de croire*. La requête judiciaire pour obtenir un mandat est entendue à huis-clos et l'installation, tout comme la désinstallation du dispositif, est secrète. Un programme d'ordinateur permettant d'effectuer ce genre de surveillance peut aussi constituer ce dispositif.

Quelles sont les données visées par les projets de loi ?

- **données sur les abonnés :**
nom, adresse, numéro de téléphone, adresse courriel, code d'identification Internet de l'utilisateur (adresse IP)
- **données de transmission :**
les données reliées à la composition de numéros, données de cheminement ou de transmission, adresse ou autres signes qui identifient l'origine, le type, la direction, la date, l'heure, la taille, la destination ou la terminaison de la télécommunication
- **données informatiques :**
toute donnée qui est sous une forme pouvant être traitée par ordinateur, ce qui représente toute donnée numérisée (carte bancaire, puces d'identification par radiofréquence, etc.)
- **données de localisation :**
données qui permettent de repérer la position d'une personne comme, par exemple, l'utilisation de cartes de crédit ou de téléphones cellulaires, d'objets munis de GPS ou d'une puce d'identification par radiofréquence (RFID)

Le Partage de renseignements entre pays

« La Convention vise beaucoup plus que la lutte contre le cybercrime : un de ses principaux objectifs est de faciliter le partage des renseignements entre les organismes d'application de la loi dans les pays participants. »

Jennifer Stoddart
Commissaire à la protection
de la vie privée du Canada

La loi C-46 permettrait à un juge d'émettre une ordonnance de préservation de données informatiques, s'il existe des *motifs raisonnables de soupçonner* qu'une infraction à la loi d'un pays étranger a été commise. Cette disposition n'exige aucune équivalence entre la loi étrangère et le droit canadien.

Cette disposition pourrait-elle permettre aux autorités d'un pays où l'avortement est un acte criminel d'obtenir les preuves nécessaires pour faire condamner une femme qui se serait faite avorter au Canada?

Des protections réduites ou inexistantes contre les saisies abusives

« *Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives* »
Charte canadienne des droits et libertés (article 8)

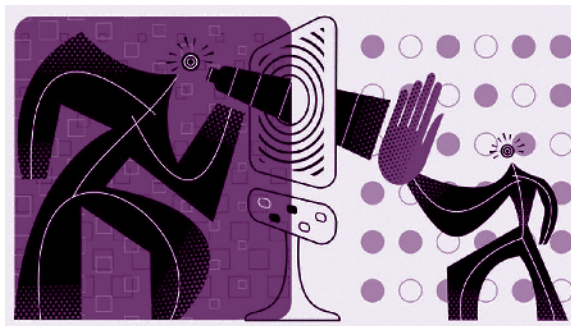
Pour procéder à une perquisition ou à une saisie l'agent doit normalement obtenir un mandat judiciaire sur la base du *motif raisonnable de croire*. Pour être raisonnable, le motif doit être fondé sur des renseignements suffisamment fiables, tel qu'une personne raisonnable en arriverait à la conclusion qu'une infraction a été commise ou sera commise, et que la saisie permettrait d'obtenir des preuves à cet

effet. Dans le cas de l'écoute téléphonique, l'atteinte à la vie privée est jugée si grave que le policier doit démontrer à un juge de la Cour supérieure que d'autres moyens moins intrusifs étaient insuffisants ou irréalisables. Par contre, le *motif raisonnable de soupçonner* est beaucoup moins exigeant car il n'est pas nécessaire de démontrer que l'information à la base du soupçon est fiable.

- Sans mandat judiciaire, les autorités pourront obtenir vos données d'abonné, alors que la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) reconnaît que ces renseignements sont de nature privée.
- Sans mandat judiciaire et sur la base du soupçon, un agent pourra demander à un fournisseur de services de conserver le contenu de toutes vos communications. C'est comme si on demandait au service des postes de photocopier toutes vos lettres... au cas où!
- Avec un mandat obtenu sur la base du simple soupçon, un agent pourra facilement obtenir que le fournisseur de services soit tenu de remettre la liste de toutes les personnes avec qui vous avez communiqué et de tous les sites Internet que vous avez visités.
- Avec un mandat sur la base du *motif raisonnable de croire*, mais moins exigeant que celui nécessaire pour l'écoute téléphonique, le contenu de vos communications pourra être intercepté.

En conclusion

- Les projets de loi C-46 et C-47 accordent aux autorités canadiennes des moyens et des pouvoirs sans précédent leur permettant de fouiller dans la vie intime des citoyen-nes et de les surveiller.
- Le gouvernement n'a pas démontré que les pouvoirs d'enquête existants étaient insuffisants.
- Dans une société démocratique, ce sont les actions du gouvernement qui doivent être transparentes et la vie privée des citoyens qui doit être protégée.



- La surveillance sur la base de simples soupçons remet en question la présomption d'innocence.
- Face à ces velléités de surveillance induite de nos communications, une certaine autocensure risque de s'installer et de brimer la liberté d'expression et de pensée.

La Ligue des droits et libertés demande le retrait des projets de loi C-46 et C-47

« La protection de la vie privée est un élément crucial d'une société libre; sans elle, il n'y a pas de réelle liberté. Présentement, le Canada se dirige dangereusement vers une société de surveillance. De plus en plus, nous réfléchissons aux situations quotidiennes en termes de « risque »; la collecte et l'utilisation de renseignements personnels – qu'on jugeait exceptionnelles jusqu'à tout récemment – deviennent monnaie courante. »

Jennifer Stoddart
Commissaire à la protection de la vie privée du Canada

LE PRÉSENT FASCICULE FAIT PARTIE D'UNE SÉRIE qui vise à informer sur différentes mesures qui nient ou limitent plusieurs droits et libertés.

À l'instar de plusieurs organisations de défense des droits partout dans le monde, la Ligue des droits et libertés s'inquiète de l'érosion des droits depuis le 11 septembre 2001 et elle a lancé une campagne de mobilisation et d'action contre ces nombreuses atteintes aux droits. Profitant d'un climat de peur et d'insécurité, souvent entretenu, plusieurs États ont étendu considérablement les pouvoirs des forces policières et leur ont confié la mise en place de vastes systèmes de fichage et de surveillance des individus.

Parmi les mesures qui portent le plus atteinte aux libertés, citons la Loi antiterroriste, le mégafichier sur les voyageurs, l'utilisation accrue de certificats de sécurité, l'introduction de documents biométriques, la collecte et le partage d'informations sur les individus, la surveillance des communications électroniques, la liste noire des voyageurs aériens. Ces nouvelles mesures bouleversent profondément notre système juridique et les valeurs consacrées dans nos chartes comme la présomption d'innocence, le droit à un procès équitable, le droit à une défense pleine et entière, le droit au silence, le droit à la vie privée et le droit d'asile.

Ces mesures se situent également dans un contexte de mondialisation néolibérale qui a eu pour effet d'augmenter les écarts entre riches et pauvres et de multiplier le nombre de personnes à statut précaire privées de droits: main d'œuvre migrante, réfugiés, sans-papiers. Par ailleurs, les individus qui contestent doivent faire face à des moyens de tout ordre mis en œuvre pour limiter la liberté d'expression, tels que les poursuites-bâillons (SLAPP) et les actions policières qui restreignent le droit de manifester.



Déjà paru dans cette série :

- Création d'une liste noire des passagers aériens au Canada
- La loi antiterroriste doit être abrogée!
- Les certificats de sécurité
- Les poursuites-bâillons (SLAPP)
- Le Taser : une arme inoffensive ?
- Les droits humains pour la liberté, l'égalité et la solidarité

Consultez notre site Internet
www.liguedesdroits.ca

Ligue des droits et libertés

65 ouest, rue des Castelnau, # 301
Montréal (Québec) H2R 2W3

Téléphone : 514 • 849 • 7717
Télécopieur : 514 • 849 • 6717

Ce fascicule a été réalisé en collaboration avec :

La Fondation
Léo-Cormier

