« Accès légal[*] » : une surveillance policière indue de nos communications

Document informatif – Janvier 2003

Ce document accompagne la **Déclaration contre le projet fédéral d'Accès légal** entérinée par la Ligue des droits et libertés du Québec (LDL), la Fédération des infirmières et des infirmiers du Québec (FIIQ), l'Association étudiante facultaire de sciences politiques et droit de l'UQAM (AFESPED-UQAM), le Centre de documentation sur l'éducation des adultes et la condition féminine (CDEACF), le Carrefour mondial de l'Internet citoyen (CMIC) et Pierrot Péladeau, chercheur spécialiste en évaluation sociale des systèmes d'information.

1. Accès légal: de quoi parle-t-on ?

Le gouvernement fédéral publiait, le 25 août 2002, un document de consultation intitulé « Accès légal ». Ce document annonce les grands principes d'une future législation permettant, d'une part, d'augmenter les capacités de surveillance électronique en les adaptant aux technologies actuelles et futures liées aux systèmes informatiques et à la téléphonie, et, d'autre part, d'obliger les fournisseurs de communications informatiques (les « serveurs» (i)), à stocker et conserver des données afin de les remettre éventuellement aux personnes chargées de l'application de la loi, incluant les fonctionnaires de certains ministères, dont le ministère du Revenu. Cette législation permettra d'intercepter le courrier électronique et d'obtenir toutes les données (acheminement, contenu) sur un abonné ou un fournisseur.

Le document part d'objectifs à première vue louables et légitimes : protection de la confidentialité et de la propriété intellectuelle, lutte contre la pornographie infantile, lutte contre le terrorisme et contre les virus informatiques. Toutefois, le projet a des conséquences dépassant de loin la simple répression de crimes particuliers et risque de nous faire basculer dans un monde où nos courriers électroniques, nos consultations et visites sur Internet, où nos moindres gestes pourraient être épiés de façon continue, où nous serions comme des microbes sous le microscope.

Comme le signale le Commissaire à la protection de la vie privée du Canada, M. George Radwanski, « Les agents de l'État du Canada ne peuvent demander à la Société canadienne des postes de photocopier l'adresse figurant sur chaque enveloppe que nous expédions, ni aux librairies de conserver un registre de tous les livres que nous achetons, et encore moins de toutes les pages de toutes les revues que nous feuilletons. Il n'y a aucune raison de pouvoir exercer de tels pouvoirs en ce qui concerne tous les courriels que quelqu'un envoie ou tous les sites Web qu'il consulte. » (ii)

---

[*] Projet présenté par le ministère de la Justice, Industrie Canada et le Solliciteur général du Canada en août 2002.

2. Mise en contexte

Le gouvernement désire adapter sa capacité de surveillance aux nouvelles technologies. « Jusqu'à récemment espionner les conversations de quelqu'un était chose relativement facile. On se branchait sur sa ligne téléphonique et on écoutait. Aujourd'hui, c'est plus compliqué. Le signal est numérisé et commuté par paquets. Il faut donc identifier quels signaux sont ceux de la cible, puis traduire ces signaux de manière intelligibles. (...) Ces communications ne passent plus uniquement par le fil du téléphone. Elles passent de plus en plus par des appareils sans fil, par la câblodistribution, par Internet. » (iii)

Ce projet de législation s'appuie également sur la volonté du Canada de se conformer à la **Convention sur la cybercriminalité**. 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. Selon certains, les négociations entre les États étaient vouées à l'impasse jusqu'aux événements du 11 septembre 2001. Le texte définitif a été adopté à Budapest, le 23 novembre 2001. Le Canada a signé la Convention le 21 novembre 2001 mais ne l'a pas encore ratifiée. La Convention invite les pays signataires à se doter de législations facilitant la surveillance électronique des communications.

3. Description plus détaillée du projet

3.1 Cybercriminalité mais aussi surveillance et enquête

La Convention ne limite pas la surveillance, la saisie de données informatiques, de même que les obligations d'entraide entre États signataires, aux infractions pénales liées à des systèmes et des données informatiques mais aussi à la collecte de preuves sous forme électronique se rapportant à une infraction pénale. Autrement dit, la Convention, tout comme le projet de législation du Canada, ne vise pas simplement la répression de crimes commis par le biais de systèmes informatiques mais aussi l'utilisation, par les personnes chargées de l'application de la loi, des systèmes informatiques à des fins générales de surveillance et d'enquête.

3.2 Obligations des « serveurs »

Les « serveurs » devraient mettre en place des dispositifs offrant aux forces de police et de sécurité nationale une capacité technique d'interception des communications. Ils devraient également conserver des données sur le trafic passant par la portion de réseau sous leur responsabilité ainsi qu'une copie des communications elles-mêmes. Ils devraient aussi produire, sur ordre d'un tribunal, les communications conservées, des données sur le trafic ou des informations sur les individus ou organismes desservis et tenir secrètes leurs collaborations aux enquêtes policières.

3.3 Interception limitée aux infractions graves ?

Le document de consultation prétend que l'interception ne pourrait s'effectuer que si l'infraction présumée possède un caractère suffisamment grave pour justifier une telle demande (p. 24).

Pourtant, les règles actuelles d'interception du Code criminel auxquelles le document se réfère vont bien plus loin que la répression d'infractions graves, tel le meurtre, la trahison, la piraterie ou l'homicide.
L'interception est aussi possible dans le cas des infractions répondant à la définition « d'infraction de terrorisme » dont le caractère excessif a été publiquement dénoncé lors de l'adoption du projet de loi C-36. Les dispositions actuelles réfèrent à plus de 115 infractions diverses, incluant des infractions hybrides (poursuivables soit comme infraction sommaire, soit comme acte criminel) comme le méfait, le vol, les menaces, la possession ou la vente de produits du tabac ou d'alcool (Loi sur l'accise), certains articles de la Loi sur les douanes, etc. On est loin d'une mesure limitée aux infractions graves. Et, paradoxalement, un acte comme la torture ne fait pas partie de la liste des infractions pour lesquelles une interception serait possible.

3.4 Élargissement des pouvoirs de surveillance et d'enquête

Normalement, pour pouvoir procéder à l'écoute électronique de conversations privées, il faut obtenir une autorisation judiciaire après avoir démontré que l'on a des motifs raisonnables et probables de croire à la commission d'une infraction. Le gouvernement souhaite un « critère moins contraignant que les motifs raisonnables ». De plus le gouvernement souhaite qu'aucune autorisation judiciaire ne soit nécessaire à la phase du début d'enquête. En fait, le gouvernement canadien désire abaisser les exigences requises actuellement, pour opérer une interception ou une surveillance électronique.

3.5 L'entraide entre les États

La Convention à laquelle réfère le projet, soulève la question des informations recueillies et transmises à un autre État pour des motifs qui dépassent les enquêtes de police usuelles. Ces motifs, souvent nébuleux, de relations internationales (élément indissociable du concept de sécurité nationale) permettent la surveillance de citoyens canadiens n'ayant rien à se reprocher afin de permettre à des organismes de surveillance étrangers de parfaire leurs banques d'informations. Ces échanges pourraient permettre à des organismes de police étrangers (ou autres agents des États), de faire ce qu'ils n'auraient pas le droit d'effectuer eux-mêmes, c'est-à-dire recueillir de l'information par le biais d'autres corps de surveillance, afin de parfaire leurs enquêtes. Notons que les garanties procédurales de protection des droits de la personne varient d'un pays à l'autre.

4. Enjeux

4.1 Atteintes à la vie privée

Ce sont des milliers de faits et gestes qui constituent la vie de chacun qui deviendront l'objet éventuel d'examen policier : en premier lieu, les sites électroniques visités par chacun, le courrier électronique reçu ou envoyé, toute 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.), mais également 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.

Selon les cas, les policiers seront à la recherche d'individus en particulier ou bien, de façon plus générale, ils interrogeront les banques de données en appliquant divers «profils» dessinés à partir de caractéristiques personnelles, de comportements ou d'habitudes. Une telle pratique fera immanquablement apparaître, à chaque fois, les noms de citoyens dont les activités personnelles les plus anodines pourront être soumises à des interprétations plus ou moins pertinentes. Et ce seront là des opérations qui se dérouleront de façon régulière, à l'insu des personnes concernées et sans que celles-ci puissent jamais rectifier la lecture qu'on aura faite des données qui les concernent.

Les risques de fuites seront augmentés de façon exponentielle alors que le nombre de serveurs a considérablement augmenté. Comment garantir que des intrus ne réussiront pas à utiliser ces masses d'informations à toutes sortes de fins commerciales ou criminelles ?

4.2 Atteintes à la liberté d'opinion, d'expression et d'association

Face à ces velléités de surveillance indue de nos communications, il y a bien des chances qu'elle en incline progressivement plusieurs à l'autocensure et brime ainsi la liberté d'expression et même celle de penser librement. Internautes et usagers du courrier électronique, en particulier, se sentiront sans cesse surveillés-es dans des activités reconnues comme privées et craindront d'éveiller les soupçons d'une police invisible.

Grâce à Internet notamment, les associations les plus diverses ont trouvé un moyen économique et rapide de communiquer. La confidentialité de ces communications nous semble aller de pair avec le droit d'association. Au fil des ans, Internet est aussi devenu un outil de sensibilisation et de mobilisation pour des citoyennes et citoyens soucieux, par exemple, de la qualité de leur environnement, de justice et de respect des droits humains. La tendance observée actuellement et qui va dans le sens de la surveillance et de la criminalisation de la dissidence, nous fait craindre que ces nouveaux pouvoirs policiers puissent être utilisés à l'encontre de ces personnes.

4.3 Enjeux de protection des citoyens canadiens face aux États étrangers

Les Canadiennes et Canadiens souhaitent-ils que les services policiers étrangers accumulent un ensemble de données personnelles sur leur compte ? Poser la question, c'est y répondre.

D'autre part, qu'arrivera-t-il quand un pays signataire demandera des informations sur un crime qui n'en serait pas un au Canada ?

Citons deux exemples :

* La pornographie infantile : il n'est pas certain que la définition de ce crime par les pays signataires soit la même que celle donnée par la Cour suprême dans l'arrêt Sharp (jurisprudence de plus de 100 pages sur les limites de l'infraction : dessins et photos de famille, œuvre artistique, etc). Récemment, aux États-Unis une loi a été invalidée en avril 2002 à cause de sa portée trop large (*Ashcroft v. Free Speech Coalition*, [2002] SCT-QL 69, No 00-795), la Cour suprême des

États-Unis jugeant que cette disposition rendrait illégale la diffusion de *Roméo et Juliette*;
* Les crimes racistes et xénophobes : en France, la Loi Gayssot criminalise le négationnisme (nier l'existence des camps de la mort nazi ou du génocide rwandais) alors qu'au Canada, la Cour suprême a invalidé des dispositions similaires du Code criminel (soit la prohibition de publier des faussetés, l'affaire Zundel), tout en prohibant la propagande haineuse (l'affaire Keegstra).

Serait-il suffisant que le Canada réprime, par exemple, la pornographie infantile, même si la portée de l'infraction est différente de celle de l'État requérant pour qu'il soit, de ce fait, tenu d'apporter son assistance à un État qui désire réprimer des actes qui ne sont pas des crimes au Canada ?

4.4 Coûts reliés au projet et enjeu d'accessibilité
Les coûts reliés à l'installation de capacités techniques d'interception et de stockage de données risquent d'être importants. Si ces coûts sont assumés par les serveurs, ils risquent d'être refilés aux utilisateurs et utilisatrices, restreignant l'accès des moins bien nantis. Si des subventions gouvernementales sont offertes aux serveurs, le coût des mesures sera aux frais de l'ensemble des contribuables.

4.5 Nouvelles modifications au Code criminel
Nous ne sommes pas encore devant un projet de loi, mais devant un simple questionnaire qui permet tout de même de comprendre les principales intentions du gouvernement. Nous savons cependant que l'on s'apprête à répéter ce que plusieurs Canadiennes et Canadiens ont considéré comme une erreur grave lors de l'adoption de C-36 : l'intégration au Code criminel, sans examen approfondi, non seulement de définitions de nouveaux délits liés à l'informatique, mais aussi de procédures policières et judiciaires, étrangères jusqu'ici à notre tradition juridique et démocratique.

4.6 Absence de contrôle démocratique
Aucune sanction spécifique n'est prévue pour réprimer les abus dans l'utilisation des nouveaux pouvoirs donnés aux policiers, au contraire, l'article 25.1 du Code criminel leur accordera l'immunité dans le cas d'une interception illégale pour fin d'enquête ! Rien ne garantit que l'utilisation de ces pouvoirs spéciaux par les divers corps de police sera scrutée de façon indépendante et aucun mécanisme d'imputabilité n'a été prévu pour que les personnes et organismes responsables de l'application de la loi aient à rendre des comptes au Parlement ou à la population !

4.7 Contexte de la « lutte anti-terroriste»
Une analyse de la Convention et du projet de législation devrait se faire en perspective avec les dispositions actuelles du Code criminel en matière de surveillance électronique, de saisies et de perquisitions, des nouvelles dispositions, des mesures et des projets de loi survenus dans la foulée des mesures antiterroristes ou « sécuritaires », comme par exemple :
a) Les nouvelles dispositions relatives au terrorisme adoptées dans le cadre du projet de loi C-36, et particulièrement :

* La définition large d'activité terroriste : ce sont non seulement des actes violents mais aussi des actes contre la « sécurité nationale » et contre la « sécurité économique »;
* Les vastes pouvoirs conférés aux forces de l'ordre, leur permettant d'interroger, surveiller, détenir (pour fins d'interrogatoire) et ficher des personnes sur lesquelles pèsent de simples soupçons d'«activités terroristes»;
* L'instauration du secret dans les procédures relatives aux procès pour terrorisme;
* Les nouvelles dispositions portant sur la sécurité nationale;
* L'allégement des conditions permettant l'écoute électronique;
* L'élargissement des pouvoirs du Centre de la sécurité de télécommunications (CST), organisme dépendant du ministère de la Défense.

b) La mise en vigueur, en février 2002, de l'article 25.1 du Code criminel (projet de loi C-24), accordant aux policiers l'immunité pour la majorité des infractions criminelles, si elles sont commises dans le cadre d'une enquête;

c) L'instauration d'un mégafichier portant sur les personnes voyageant par avion à l'extérieur du pays. Le ministère du Revenu a déjà annoncé que, d'ici 2004, ce sont toutes les personnes utilisant le train, l'autobus et le bateau qui seront progressivement fichées (loi S-23, Modification à la Loi des douanes);

d) Le projet de loi C-17, en voie d'adoption (Projet de loi sur la sécurité publique), octroyant à la GRC et au Service canadien de renseignement sur la sécurité (SCRS), un accès sans restriction aux informations que les sociétés aériennes obtiennent sur leurs passagers. De plus, la GRC serait habilitée à utiliser ces renseignements pour repérer toute personne à l'égard de laquelle un mandat aurait été délivré même dans le cas d'une infraction pénale qui serait sans aucun rapport avec le terrorisme, la sécurité des transports ou la sécurité nationale;

e) Le projet du ministre de la Citoyenneté et de l'Immigration, Monsieur Denis Coderre, d'une carte d'identité canadienne, qui comporterait cette fois des données biométriques, comme les empreintes digitales ou l'image de l'iris;

f) L'annonce en octobre 2002 de la création d'une autre banque de données qui, elle, contiendra les photos numérisées des 10 millions de Canadiens et de Canadiennes qui détiennent un passeport.

En elles-mêmes, ces mesures sont déjà démesurées. Or, ces capacités de surveillance seront multipliées par le couplage de données entre les différents fichiers d'informations accumulées par les services policiers et des ministères. Et elles le seraient encore plus par un accès total aux informations qui seront produites et échangées par des systèmes n'ayant, a priori, rien à voir avec l'antiterrorisme.

Songeons à l'accès aux registres et aux communications des services d'accès à Internet, des services de téléphonie cellulaire, des réseaux locaux de communication sans fil dans les entreprises, universités et hôpitaux. Songeons à l'accès aux réseaux inter-entreprises comme ceux de guichets bancaires ou

inter-organismes publics comme ceux de dossiers santé électroniques supportés ou non par des cartes santé à microprocesseur. Songeons aussi aux systèmes de commerce électronique ou de services électroniques aux citoyens ainsi qu'aux dispositifs devant les faciliter comme ceux d'identification électronique ou biométrique des individus. Si le projet « Accès légal » est adopté, toutes ces activités pourraient ainsi s'intégrer en un système de surveillance totale de la population.

5. Conclusion

Une consultation fort discrète comme celle que le gouvernement du Canada a entreprise cet automne et qui s'est terminée le 16 décembre 2002 est insuffisante vu l'ampleur des enjeux. Le projet annoncé est sans précédent et aura un impact important sur toute la société, son fonctionnement et l'ensemble des relations entre ses différentes composantes, et pourtant, nous constatons l'absence de débat public sur la question.

Depuis plus d'un an maintenant, nous assistons à l'adoption d'une série de mesures mettant en péril les libertés civiles au Canada (C-36, C-17, etc.). « Accès légal» s'ajoute à ces mesures. Leurs effets s'additionnent et créent un environnement de plus en plus contrôlé.

Tout comme M. George Radwanski, nous croyons que la démonstration de la nécessité d'une telle intrusion dans la vie privée des Canadiennes et des Canadiens n'a pas été faite. Nous pressons donc le Gouvernement de surseoir à son projet sur l' «Accès légal».

---

i Les serveurs privés ou publics y compris possiblement les institutions du milieu de l'enseignement, de la santé, etc., qui offrent ce service à leurs employés-es, à leurs étudiants et étudiantes, etc.

ii Extrait de la lettre que le Commissaire à la protection de la vie privée du Canada, George Radwanski, a envoyée au ministre de la Justice et Procureur général du Canada, Monsieur Martin Cauchon, à Monsieur Wayne Easter, Solliciteur général du Canada, ainsi qu'à l'honorable Allan Rock, ministre de l'Industrie, au sujet des propositions relatives à l'«accès légal», 25 novembre 2002 : www.privcom.gc.ca/media/le_021125_f.asp

iii Pierrot Péladeau, «Vers une surveillance de tous, sur tout, par tous?», *Direction informatique*, novembre 2002, Publications Transcontinental.

Pour plus d'information sur l'accès légal, rendez-vous à la section sur l'accès légal du site du Carrefour mondial de l'Internet citoyen : www.globalcn.org/fr/accueil.ntd?sort=1.6.9