Résumé législatif **LS-519F**

PROJET DE LOI C-74 : LOI SUR LA MODERNISATION DES TECHNIQUES D'ENQUÊTE

Dominique Valiquet
Division du droit et du gouvernement

Le 21 décembre 2005

Bibliothèque du Parlement
Library of Parliament

Service d'information et de recherche parlementaires

HISTORIQUE DU PROJET DE LOI C-74

CHAMBRE DES COMMUNES		SÉNAT	
Étape du projet de loi	**Date**	**Étape du projet de loi**	**Date**
Première lecture :	15 novembre 2005	Première lecture :	
Deuxième lecture :		Deuxième lecture :	
Rapport du comité :		Rapport du comité :	
Étape du rapport :		Étape du rapport :	
Troisième lecture :		Troisième lecture :	

Sanction royale :

Lois du Canada

N.B. Dans ce résumé législatif, tout changement d'importance depuis la dernière publication est indiqué en **caractères gras**.

Renseignements sur l'historique du projet de loi :
Peter Niemczak

THIS DOCUMENT IS ALSO PUBLISHED IN ENGLISH

TABLE DES MATIÈRES

Page

Page

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

PROJET DE LOI C-74 : LOI SUR LA MODERNISATION DES TECHNIQUES D'ENQUÊTE*

CONTEXTE

A. Accès légal

Le projet de loi C-74 a été déposé le 15 novembre 2005 à la Chambre des communes par la ministre de la Sécurité publique et de la Protection civile (la ministre). Il traite de certains aspects bien précis du régime de l'accès légal. L'accès légal constitue une technique d'enquête dont se servent les organisations d'application de la loi et les organismes chargés de la sécurité nationale(1). Il s'agit de l'interception de communications(2) et de la saisie de données(3) autorisées par la loi.

B. Objets du projet de loi

Le projet de loi crée la *Loi sur la modernisation des techniques d'enquête* (LMTE) qui vise deux objectifs. Premièrement, contraindre les personnes qui fournissent des

---

* Avertissement : Par souci de clarté, les propositions législatives du projet de loi décrit dans le présent résumé législatif sont énoncées comme si elles avaient déjà été adoptées ou étaient déjà en vigueur. Il ne faut pas oublier, cependant, qu'un projet de loi peut faire l'objet d'amendements au cours de son examen par la Chambre des communes et le Sénat, et qu'il est sans effet avant d'avoir été adopté par les deux chambres du Parlement, d'avoir reçu la sanction royale et d'être entré en vigueur.

(1) Par souci de concision, les références, dans le présent texte, aux « organismes d'application de la loi » s'entendent également des organismes chargés de la sécurité nationale, sauf si le contexte indique clairement le contraire.

(2) Appelée communément « écoute électronique », cette technique est très utile pour enquêter sur divers crimes, notamment les infractions reliées aux drogues. Pour ce qui est du nombre exact de condamnations obtenues grâce, entre autres, à l'écoute électronique, voir Sécurité publique et Protection civile Canada, *Rapport annuel sur la surveillance électronique – 2004*, figures 3 et 4 (http://www.psepc-sppcc.gc.ca/ abt/dpr/le/elecsur-fr.asp).

(3) Lors d'une perquisition.

services de télécommunication (les « télécommunicateurs ») à posséder la capacité d'intercepter les communications sur leurs réseaux. Deuxièmement, permettre aux organismes d'application de la loi d'avoir accès, sur demande, à certains renseignements de base identifiant les abonnés des services de télécommunication.

D'entrée de jeu, il est primordial de noter que l'interception de communications privées demeure conditionnelle à l'obtention d'une autorisation judiciaire(4). Le projet de loi ne change en rien cet état de fait. Le premier objectif concerne uniquement la *capacité technique* des appareils de transmission à pouvoir intercepter les communications. Ainsi, les organismes d'application de la loi pourront intercepter tant les communications par téléphone traditionnel que celles utilisant les nouvelles technologies comme Internet. Mais l'interception d'une communication Internet, à l'instar d'une communication téléphonique, exigera aussi de présenter une demande à un juge.

Ensuite, le deuxième objectif du projet de loi ne concerne que certains *identificateurs associés à l'abonné*, comme son nom et son adresse. Par conséquent, le système spécial mis en place pour donner accès à ce genre de renseignements ne comprend pas les sites Web visités ou encore le contenu d'un courrier électronique. Pour obtenir ces informations, les organismes d'application de la loi devront – comme pour tous renseignements autres que les identificateurs spécifiés par le projet de loi et la réglementation – se munir d'un mandat ou d'une autorisation judiciaire.

Finalement, si le projet de loi donne la définition de certains termes et fournit les grandes lignes du nouveau régime, les règlements à venir apporteront les détails nécessaires et préciseront les normes techniques.

C. Fondements du projet de loi

1. Consultations

Depuis 1995, l'Association canadienne des chefs de police (ACCP) réclame l'adoption d'une loi obligeant tous les télécommunicateurs à se munir de moyens techniques

---

(4) Remarquons, toutefois, qu'une autorisation judiciaire n'est pas nécessaire si l'interception est effectuée par le Centre de la sécurité des télécommunications (CST) dans le cadre de la partie V.1 de la *Loi sur la Défense nationale*, L.R. 1985, ch. N-5. En revanche, d'autres mesures de protection sont prévues.

permettant aux forces de l'ordre d'intercepter les communications sur leurs réseaux(5). Et si l'initiative de réforme a pris naissance dans les années 1990 – soit avant les attaques du 11 septembre 2001 –, le ministère de la Sécurité publique et de la Protection civile avance que le projet de loi est nécessaire afin de lutter plus efficacement contre le terrorisme(6). Le Ministère évoque aussi la lutte au crime organisé.

Suivant l'élaboration d'un cadre de travail en 2000, des représentants de Justice Canada, d'Industrie Canada et du Solliciteur général du Canada ont procédé à des consultations publiques qui se sont déroulées du mois d'août au mois de décembre 2002. Après avoir reçu plus de 300 observations de la part de services de police, d'intervenants de l'industrie, de groupes de défense des droits civiques et de particuliers, un résumé des résultats des consultations a été publié en 2003. En 2005, une série de réunions avec les intéressés a suivi.

2. Nouvelles technologies

Les Canadiens ont accès à un nombre toujours croissant de nouvelles technologies de communication. Plus de la moitié des ménages possède un téléphone cellulaire et a accès à Internet à la maison(7).

Selon les organismes d'application de la loi, les nouvelles technologies – comme les réseaux de données sans fil et le système vocal sur l'Internet(8) – représentent souvent des obstacles à l'interception légale des communications(9). Seraient ainsi créées des « zones

---

(5) Sécurité publique et Protection civile Canada, *Loi sur la modernisation des techniques d'enquête – Chronologie*, 15 novembre 2005 (http://www.sgc.gc.ca/media/bk/2005/bk20051115-1-fr.asp).

(6) Séance d'information technique tenue par Sécurité publique et Protection civile Canada le 15 novembre 2005.

(7) Par ailleurs, « les Canadiennes et les Canadiens envoient plus de 2,7 millions de messages alphabétiques par jour » (Commissariat à la protection de la vie privée du Canada, « Réponse à la consultation du gouvernement sur l'accès légal », 5 mai 2005, http://www.privcom.gc.ca/information/pub/sub_la_050505_f.asp).

(8) Voix sur IP ou « Voice over Internet Protocol » (VoIP). Pensons aussi aux nouvelles options perfectionnées de service et les nouvelles caractéristiques d'appel; aux communications par satellites; aux téléavertisseurs et aux assistants numériques personnels (ANP) qui emploient des algorithmes protégés; aux réseaux superposés de transmission de données à haute vitesse qui permettent la transmission sans fil de données par paquets.

(9) Nevis Consulting Group Inc. (dir.), *Résumé des mémoires présentés dans le cadre de la Consultation sur l'accès légal*, 28 avril 2003, p. 5, 19 et 36. Entre autres, l'incapacité de déchiffrer les messages codés et l'absence de protocoles uniformes en matière de partage de données causeraient problème.

sûres » où les groupes criminels pourraient agir sans être détectés. Avec notamment la déréglementation du marché des télécommunications, la complexité accrue des réseaux téléphoniques rendrait le travail des enquêteurs plus difficile et occasionnerait, par le fait même, des délais dans l'identification des suspects.

Le projet de loi vient donc imposer une capacité d'interception aux télécommunicateurs, et ce, quelle que soit la technologie qu'ils utilisent. Il vise tous les types de technologies actuelles et futures.

3. International(10)

Certains pays, notamment les États-Unis, le Royaume-Uni, la France, l'Allemagne, l'Australie, la Nouvelle-Zélande et l'Afrique du Sud, ont adopté des lois sur l'interception des communications transmises par le truchement des nouvelles technologies.

Le 23 novembre 2001, le Canada a signé la Convention sur la cybercriminalité du Conseil de l'Europe. La Convention criminalise certaines infractions commises à l'aide de systèmes informatiques(11) et met en place des outils juridiques permettant d'enquêter sur les activités des criminels qui utilisent les nouvelles technologies(12). La coopération internationale étant essentielle dans un domaine où le crime ne connaît aucune frontière, ce traité a aussi comme objectif de faciliter le partage de renseignements entre les organismes d'application de loi des différents pays.

Le projet de loi C-74 constitue ainsi une façon de doter le Canada d'une loi semblable à celles d'autres pays et de mettre en œuvre certaines mesures de la Convention sur la cybercriminalité(13).

---

(10) Cet aspect fait l'objet d'une analyse plus détaillée dans le cadre d'une publication distincte.

(11) Entre autres, la fraude sur Internet, la pornographie enfantine et les infractions relatives aux virus informatiques. Un protocole additionnel s'attaque à la propagande haineuse.

(12) Il s'agit notamment des ordonnances de conservation et de production (incluant une injonction de produire les « données relatives aux abonnés »).

(13) Afin de ratifier la Convention, des modifications au *Code criminel* seront aussi nécessaires, notamment afin d'inclure des ordonnances de conservation et de production de même qu'élargir l'infraction relative aux virus informatiques.

D. Les mesures absentes du projet de loi

Plusieurs mesures proposées lors des consultations n'ont pas été retenues. La création d'une base de données nationale de même que les obligations de stockage et de « connaître ses clients » continueront certainement à recevoir de fortes oppositions, notamment de la part des défenseurs de la vie privée. Il n'est toutefois pas exclu que certaines mesures – comme les ordonnances de conservation et de production – fassent l'objet de projets de loi subséquents.

1. Obligation de stockage et base de données nationale

Le projet de loi ne contraint pas les télécommunicateurs à recueillir et conserver des renseignements sur leurs abonnés. Les fournisseurs de services ne seront donc pas dans l'obligation de collecter et conserver systématiquement les activités de navigation sur Internet des Canadiens.

Par ailleurs, une base de données nationale comprenant les informations sur les abonnés des services de télécommunication, tant les identificateurs – comme les noms et adresses – que les activités de communication, ne sera pas mise sur pied.

2. « Connaître sa clientèle »

Aucune obligation imposée aux télécommunicateurs de vérifier l'identité de leurs abonnés n'est prévue au projet de loi[(14)]. Ainsi, les services anonymes, comme les cartes téléphoniques prépayées, demeurent légaux.

3. Ordonnance de conservation

Il s'agit d'une ordonnance judiciaire, délivrée sur la base de motifs raisonnables, en vigueur pour la durée nécessaire à l'organisme d'application de la loi pour obtenir un mandat de perquisition ou une ordonnance de production. Elle représente donc une mesure accélérée afin de protéger des renseignements qui peuvent facilement être détruits ou modifiés dans l'intervalle.

---

(14) Cette mesure n'est pas incluse bien que les organismes d'application de la loi considèrent que les services cellulaires prépayés, les cartes d'accès Internet, les cafés Internet et les terminaux d'accès à Internet dans les bibliothèques publiques compliquent la tâche des enquêteurs (*Mémoires sur l'accès légal* (2003), p. 18).

Elle enjoint au télécommunicateur de conserver des renseignements à propos d'une transaction particulière ou d'une personne visée. La conservation doit se faire dans le cadre d'enquêtes et vise des données qui sont déjà stockées(15).

Les institutions fédérales responsables des consultations ont aussi proposé qu'un organisme d'application de loi, face à une situation d'urgence, puisse imposer au télécommunicateur de conserver des données sans avoir obtenu préalablement l'autorisation d'un juge(16). Cette mesure ne serait toutefois valide que pour une courte période.

Absente du projet de loi C-74, l'ordonnance de conservation pourrait être introduite sous forme d'une modification au *Code criminel* (le *Code*)(17).

4. Ordonnance spécifique de production

Ce type d'ordonnance judiciaire, qui exige aussi la présence de motifs raisonnables afin d'être délivrée, est semblable à un mandat de perquisition. Toutefois, au lieu que l'organisme d'application de la loi se rende sur place pour obtenir les renseignements recherchés, c'est le télécommunicateur qui produit l'information demandée. Les organismes d'application de la loi peuvent alors obtenir des documents se trouvant dans un autre pays.

Le *Code* prévoit une procédure pour obtenir une ordonnance de production générale, c'est-à-dire qui s'applique peu importe le type de renseignement qu'un organisme d'application de la loi recherche(18). La délivrance d'une telle ordonnance est basée sur l'existence de motifs raisonnables *de croire* qu'une infraction a été commise (critère exigeant)(19). Une ordonnance de production spécifique est aussi prévue pour obtenir un registre

---

(15) Une ordonnance de conservation n'oblige pas un télécommunicateur à recueillir et stocker certaines données concernant tous ses abonnés.

(16) Ministère de la Justice, Industrie Canada et Solliciteur général du Canada, *Accès légal – Document de consultation*, 25 août 2002, p. 17.

(17) L.R. 1985, ch. C-46.

(18) Article 487.012 du *Code*. Une telle ordonnance est également prévue par la *Loi sur la concurrence*, L.R. 1985, ch. C-34 (al. 11(1)*b*)).

(19) Alinéa 487.012(3)*a*) du *Code*.

des appels téléphoniques[20]. La délivrance de cette ordonnance est fondée sur l'existence de motifs raisonnables de *soupçonner* qu'une infraction a été ou sera commise (critère moins exigeant)[21].

Une proposition avancée lors des consultations de 2002 consistait à créer une ordonnance de production pour obtenir des télécommunicateurs les données indiquant l'itinéraire des communications (« données de transmission »)[22]. À l'instar de l'ordonnance relative aux registres des appels téléphoniques, l'ordonnance de production proposée aurait pu être délivrée sur la base du critère moins exigeant, soit la présence de motifs raisonnables de soupçonner[23]. Le projet de loi C-74 ne contient pas une telle ordonnance.

5. Courrier électronique

Le projet de loi ne met pas fin au débat entourant le traitement du courrier électronique. Il ne précise pas, en effet, quelles règles s'appliquent en la matière : la partie VI du *Code*[24] ou les dispositions relatives aux mandats de perquisition[25].

---

(20) Paragraphe 492.2(2) du *Code*.

(21) *Ibid*. Le *Code* utilise aussi le critère des motifs raisonnables de soupçonner dans le cas de l'ordonnance de production d'informations bancaires (par. 487.013(1) et (4)) et dans le cas du mandat pour installer un dispositif de localisation (par. 492.1(1)).

(22) On utilise aussi l'expression « données relatives au trafic ». Essentiellement, ce sont des données qui indiquent l'origine, la destination, la date, l'heure, la durée et le volume d'une télécommunication.

(23) Ne révélant pas le contenu de la communication, on considère que la collecte des données de transmission constitue une intrusion de la vie privée moins importante. C'était du moins le point de vue des institutions fédérales responables des consultations de 2002 (*Accès légal – Document de consultation* (2002), p. 14). Voir aussi Conseil de l'Europe, *Convention sur la cybercriminalité – Rapport explicatif* (http://conventions.coe.int/Treaty/FR/Reports/Html/185.htm).

(24) Articles 183 et suivants du *Code*.

(25) Le régime relatif aux saisies et perquisitions est prévu, notamment, aux art. 487 et suivants du *Code* ainsi qu'aux art. 15 et 16 de la *Loi sur la concurrence*. Par ailleurs, le même type de questionnement peut aussi être soulevé à l'égard du clavardage et de la messagerie instantanée. De plus, on se demande si des règles différentes devraient s'appliquer suivant le lieu où se trouve le message électronique. Par exemple, d'une part, une organisation policière devrait obtenir un mandat de perquisition pour saisir un courriel en transit chez le fournisseur Internet de l'auteur ou du destinataire du message. D'autre part, elle devrait respecter les règles de la partie VI pour intercepter un courriel dans la boîte de réception de l'auteur ou du destinataire.

Le régime de la partie VI est plus exigeant que celui établi relativement aux mandats de perquisition(26). Il permet aux organisations policières d'intercepter une « communication privée »(27). Si un courriel constitue bel et bien une télécommunication, il n'est pas certain que son auteur puisse s'attendre raisonnablement à ce que seulement son destinataire en prenne connaissance(28). En effet, un tel message peut être facilement intercepté(29). En revanche, pourquoi établir une différence avec une télécopie ou une communication par téléphone? D'autant plus qu'un courrier électronique peut renfermer diverses informations et contenir des renseignements personnels délicats.

DESCRIPTION ET ANALYSE

Des règles concernant l'accès légal sont prévues dans plusieurs lois fédérales, notamment au *Code criminel*, dans la *Loi sur le Service canadien du renseignement de sécurité*(30) et dans la *Loi sur la Défense nationale*(31). Le paragraphe 2(2) du projet de loi

---

(26) La partie VI du *Code* contient des mesures de protection additionnelles. Afin d'autoriser l'interception d'une communication privée, un juge devra notamment être convaincu que l'interception servirait l'administration de la justice (al. 186(1)*a*) du *Code*) et qu'il est véritablement nécessaire d'y recourir, car il n'existe aucune autre méthode d'enquête raisonnable dans les circonstances [al. 186(1)*b*) du *Code*. Il s'agit de l'exigence de nécessité. Sur cet aspect, voir la décision de la Cour suprême *R.* c. *Araujo*, [2000] 2 R.C.S. 992. Observons par ailleurs que l'exigence de nécessité ne s'applique pas lorsque l'interception concerne une infraction de terrorisme ou le crime organisé (par. 186(1.1) du *Code*)]. De plus, uniquement certaines infractions spécifiées peuvent justifier une interception par une organisation policière [la liste des infractions se trouve à l'art. 183 du *Code*. En ce qui concerne l'interception de communications avec le consentement de l'auteur ou du destinataire (surveillance « participative » ou « consensuelle »), il s'agit toutefois de toute infraction prévue au *Code* ou à toute autre loi fédérale (al. 184.2(2)*a*))].

(27) L'article 183 du *Code* définit ainsi une « communication privée » : « Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine. » L'art. 35 de la *Loi d'interprétation*, L.R. 1985, ch. I-21, donne la définition d'une télécommunication : « La transmission, l'émission ou la réception de signes, signaux, écrits, images, sons ou renseignements de toute nature soit par système électromagnétique, notamment par fil, câble ou système radio ou optique, soit par tout procédé technique semblable. »

(28) Robert W. Hubbard, Peter M. Brauti, Scott K. Fenton, *Wiretapping and Other Electronic Surveillance*, Canada Law Book, Aurora, n° 11, septembre 2005, p. 1-10.1 et 6-22.4.

(29) Voir *R.* c. *Weir*, [1998] 8 W.W.R. 228 (Alta, Banc de la Reine).

(30) L.R. 1985, ch. C-23.

(31) Comme nous l'avons dit ci-dessus, la *Loi sur la concurrence* contient également des dispositions portant sur les perquisitions, les saisies et les ordonnances de production.

précise, pour plus de certitude, que les organismes d'application de la loi conservent les pouvoirs conférés par ces lois(32). Le projet de loi C-74 vient permettre aux organismes d'application de la loi d'exercer ces pouvoirs peu importe la technologie utilisée par les télécommunicateurs (capacité d'interception). Il prévoit aussi une procédure spéciale afin que certains organismes aient accès à des informations de base concernant les abonnés des services de télécommunication (renseignements sur les abonnées). En plus de traiter de ces deux aspects centraux du projet de loi, notre présentation abordera la question des pénalités et des exemptions. Cependant, nous n'examinerons pas en détail chacun des 59 articles du projet de loi.

A. Capacité d'interception

1. La situation actuelle

Il n'existe, à l'heure actuelle, aucune loi canadienne contraignant tous les télécommunicateurs à utiliser des appareils qui possèdent une capacité d'intercepter les communications. Seuls les titulaires de licence qui utilisent les fréquences radio pour des systèmes de téléphonie vocale sans fil(33) doivent, depuis 1996, détenir des installations permettant de telles interceptions(34). Il n'existe aucune obligation semblable pour les autres télécommunicateurs.

2. La situation en vertu du projet de loi

C'est cette absence de standard dans la capacité d'interception des télécommunicateurs à laquelle le projet de loi veut remédier. Il oblige tous ceux qui fournissent des services de télécommunications, par exemple les fournisseurs de services Internet (FSI), à

---

(32) Voir aussi l'art. 21 du projet de loi.

(33) On parle alors de « services de communications personnelles » (SCP) qui désigne essentiellement les téléphones numériques sans fil.

(34) Cette condition est imposée par Industrie Canada lors de la délivrance des licences de spectre en vertu de la *Loi sur la radiocommunication* (L.C. 1991, ch. 11). Les normes d'interception sont indiquées dans les *Normes d'application du Solliciteur Général sur l'interception licite des télécommunications* (révisées en novembre 1995). Voir Kristen Embree, « Lawful Access : A Summary of the Federal Government's Recent proposals – Part I », (2005-2006) 6 *I.E.C.L.C.*, mai 2005, p. 18, et le site Web d'Industrie Canada, « Gestion du spectre et télécommunications – Services de communications personnelles » (http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/fr/h_sf02092f.html).

posséder des appareils[35] permettant aux organismes d'intercepter, après avoir obtenu une autorisation judiciaire, les communications qui y sont acheminées. Le projet de loi s'applique donc, à l'exception des exemptions prévues, à tous les télécommunicateurs qui opèrent une installation de transmission au Canada[36].

Par ailleurs, l'obligation de posséder une capacité d'interception uniforme vise autant les données de transmission que celles relatives au contenu même de la communication (art. 2[37], 6 et 7 du projet de loi). Un FSI doit ainsi utiliser des appareils permettant aux organismes d'application de la loi de mettre la main sur, par exemple, d'une part, les adresses courriel et de protocole Internet (adresse IP[38]) des abonnés, la date et l'heure des communications ainsi que le type de fichier transmis (données de transmission) et d'autre part, les pages Web visitées de même que la substance des messages (données relatives au contenu).

3. Moment de prise d'effet des obligations

Le projet de loi n'impose pas aux télécommunicateurs de satisfaire aux normes techniques sur la capacité d'interception dans l'immédiat. Il exige plutôt de conserver leur capacité d'interception existante (art. 8), et ce, même lorsqu'ils fourniront de nouveaux services (art. 9).

En revanche, les télécommunicateurs devront se conformer aux nouvelles normes techniques d'interception lorsqu'ils effectueront une mise à jour de leurs réseaux. C'est-à-dire, au moment de l'acquisition d'un nouvel appareil de transmission (art. 10) ou lors de l'installation d'un nouveau logiciel (art. 11 du projet de loi). Même dans ces cas, le projet de loi prévoit une période de transition de 12 mois (art. 58). Ainsi, un télécommunicateur qui, par exemple, installe un nouveau logiciel après l'entrée en vigueur du projet de loi ne devra respecter les normes techniques qu'à la première date d'anniversaire de la loi. Une nouvelle entreprise de télécommunication qui entre sur le marché après cette date devra satisfaire aux exigences techniques sur la capacité d'interception (art. 10 du projet de loi).

---

(35) La réglementation précisera les standards techniques.

(36) Plusieurs sociétés qui fournissent des services de télécommunication au Canada n'y possèdent toutefois qu'un bureau, l'ensemble de leurs installations étant situé aux États-Unis.

(37) Définissant les termes « communication » et « données de transmission ».

(38) Cette adresse peut être fixe ou différer à chaque branchement (adresse IP dynamique).

Toutefois, le ministre a le pouvoir d'ordonner, par arrêté, à un télécommunicateur qu'il se munisse de la capacité d'intercepter des communications conformément aux normes techniques avant qu'il ne procède à une mise à niveau (al. 15(1)*d*) et *e*)). Soulignons, par ailleurs, que le ministre devra verser une indemnité qu'il estime suffisante pour couvrir les dépenses engagées afin de se conformer à un arrêté, et ce, peu importe l'objet de l'arrêté (par. 15(3) du projet de loi).

4. Les obligations

a. Obtempérer aux demandes et fournir l'information

Une fois qu'un organisme d'application de la loi aura une autorisation judiciaire en main, le télécommunicateur devra obtempérer à toute demande se rapportant à l'interception des communications (par. 6(1) du projet de loi). En vertu de la politique de réglementation établie par le ministère de la Sécurité publique et de la Protection civile, le télécommunicateur devra permettre aux organismes d'application de la loi d'intercepter des communications dès que possible après la réception d'un avis écrit ou oral, et au plus tard, dans :

- les deux jours ouvrables;
- les 30 minutes à huit heures en présence de circonstances exceptionnelles[39].

Le télécommunicateur devra fournir la communication interceptée dans la forme précisée par règlement (al. 6(1)*a*) et par. 6(3)). En outre, il est tenu de procurer aux organismes d'application de la loi, sur demande, des renseignements concernant les installations et services de télécommunication qu'il offre à sa clientèle en général ou à la personne visée par une autorisation judiciaire d'interception (al. 6(1)*c*) et art. 23 du projet de loi).

b. Prêter assistance

Le télécommunicateur a l'obligation légale de prêter assistance à tout organisme d'application de la loi afin d'évaluer les installations de télécommunication (art. 24 du projet de

(39) Par exemple, lors d'une situation urgente menaçant la sécurité nationale.

loi)[40]. Par exemple, il pourra confirmer que les appareils interceptent effectivement les communications et qu'il s'agit bien des communications de la personne visée par l'autorisation judiciaire.

Il doit dresser une liste contenant les noms de ses employés qui pourront fournir leur assistance. Cette liste sera disponible, sur demande, aux organismes d'application de loi et ceux-ci pourront tenir une enquête afin d'évaluer la sécurité des employés qui y sont mentionnés (art. 27 du projet de loi).

c. Confidentialité

Tout processus d'interception doit rester confidentiel (al. 6(1)*d*))[41]. Les télécommunicateurs seront donc tenus de se conformer aux mesures réglementaires afin de garantir la sécurité du contenu de la communication interceptée, des données relatives au trafic et de l'identité des personnes et des organismes impliqués.

d. Interception en temps réel

C'est l'alinéa 7*a*) du projet de loi qui prévoit, de façon générale, que les télécommunicateurs devront posséder la capacité d'intercepter les communications conformément aux normes techniques qui seront établies par les règlements à venir.

La collecte en temps réel des données de transmission est une importante mesure d'enquête permettant, entre autres, d'identifier la source de l'intrusion ou de la diffusion. D'après la politique de réglementation, si un télécommunicateur ne possède pas la capacité d'intercepter de telles données en temps réel, il doit, au moins, pouvoir les intercepter une seconde après l'interception du contenu de la communication.

---

(40) On retrouve notamment une ordonnance d'assistance générale à l'art. 487.02 du *Code*. Elle s'applique à tout acte autorisé dans le cadre d'une autorisation d'interception ou d'un mandat de perquisition.

(41) Par ailleurs, les corps policiers qui ont procédé à une interception en vertu de la partie VI du *Code* ont l'obligation d'aviser par écrit la personne qui a fait l'objet de l'interception. Le délai habituel de 90 jours (par. 196(1)) a été repoussé à trois ans dans le cas du crime organisé et des infractions de terrorisme (par. 196(5)). Cette obligation ne s'applique pas aux interceptions effectuées par le Service canadien du renseignement de sécurité ou le Centre de la sécurité des télécommunications.

e. Isoler la communication

Une autorisation judiciaire d'intercepter les communications visera une ou plusieurs personnes en particulier. Le télécommunicateur doit alors pouvoir séparer les communications de la personne visée par l'autorisation de celles des autres utilisateurs (sous-al. 7*b*)(i) du projet de loi). Il doit aussi détenir la capacité de dissocier les données de transmission de celles relatives au sens de la communication (sous-al. 7*b*)(ii)).

f. Mettre en corrélation

Un télécommunicateur doit posséder la capacité technique de faire exactement l'opposé de ce qui a été énoncé précédemment. C'est-à-dire réunir et faire des liens entre les données relatives au trafic et le contenu d'une communication interceptée (al. 7*c*) du projet de loi). Ainsi, l'organisme d'application de la loi pourra, par exemple, établir une connexion entre l'infraction commise et une adresse IP.

g. Interceptions simultanées

Les télécommunicateurs sont tenus de permettre aux organismes d'application de la loi d'intercepter les communications de plusieurs utilisateurs qui sont transmises au même moment (al. 7*d*) du projet de loi). Les règlements fixeront des limites minimales et maximales[(42)] du nombre d'interceptions simultanées que devront pouvoir supporter les installations de télécommunication (sous-al. 7*d*)(ii) et art. 13 du projet de loi). Par arrêté, le ministre pourra toutefois ordonner à un télécommunicateur de prendre des mesures pour accroître le nombre d'interceptions simultanées au-delà de la limite maximale (al. 15(1)*b*) du projet de loi).

h. Chiffrement

Présentement, les fournisseurs de services de communications numériques sans fil ont l'obligation, en vertu de conditions imposées dans les permis d'exploitation, de donner accès aux communications en clair aux organismes d'application de la loi. Le projet de loi étend cette

(42) La politique de réglementation prévoie un minimum de deux interceptions simultanées, tandis que le maximum dépend du nombre d'abonnés.

obligation à toutes les technologies (al. 6(1)*b*)). Si les mesures de protection d'une communication – comme le chiffrement ou le codage – ont été apposées par une autre personne que le télécommunicateur et qu'il est dans l'impossibilité de les défaire, il devra alors prêter toute l'assistance raisonnable aux organismes d'application de la loi en vue de les défaire (sous-al. 6(1)*b*)(ii) et par. 6(2))[43].

5. Rapport

Tous les télécommunicateurs doivent présenter au ministre un rapport indiquant leur capacité de répondre aux exigences d'interception posées par le projet de loi (article 28 du projet de loi)[44]. Ils devront fournir un tel rapport dans les six mois de l'entrée en vigueur du projet de loi, lors de l'acquisition d'un appareil de transmission ou à tout moment lorsque le ministre l'exigera.

B. Renseignements sur les abonnés

1. La situation actuelle

Actuellement, les organismes d'application de la loi doivent être munis d'un mandat ou d'une ordonnance judiciaire afin de contraindre les télécommunicateurs à leur transmettre les renseignements personnels qu'ils détiennent sur leurs clients[45].

2. La situation en vertu du projet de loi

Le projet de loi met en place un régime spécial permettant à certaines personnes désignées de contraindre, sans mandat ni ordonnance judiciaire, un télécommunicateur à leur fournir des informations de base concernant un de leurs abonnés. Des mesures de protection encadrent cette demande de renseignements.

---

(43) Au plan international, voir l'Arrangement de Wassenaar (conclu en 1996) concernant, entre autres, le contrôle des technologies à double usage (http://www.wassenaar.org/).

(44) Ceux qui satisferont à toutes les exigences législatives pourront, alternativement, fournir une attestation à cet effet.

(45) Voir l'al. 7(3)*c*.1) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ), L.C. 2000, ch. 5. Concernant la protection des renseignements personnels, détenus par une entreprise, qui ne révèlent pas de détails intimes sur le mode de vie ou les choix personnels des clients, voir *R.* c. *Plant*, [1993] 3 R.C.S. 281 (décision examinée dans un arrêt plus récent de la Cour suprême : *R.* c. *Tessling*, [2004] 3 R.C.S. 432).

3. La demande de renseignements

a. Types de renseignements visés

Les renseignements qui sont couverts par le régime spécial sont strictement limités. Le ministère de la Sécurité publique et de la Protection civile fait un parallèle avec les informations que l'on trouve dans un annuaire téléphonique.

Il s'agit uniquement des coordonnées de base identifiant un abonné, comme son nom, son adresse IP, son adresse de courrier électronique, son numéro de téléphone, son numéro de cellulaire ou tout numéro unique rattaché à un tel appareil(46) (par. 17(1) du projet de loi). Ces renseignements sont bien souvent indispensables aux organismes d'application de la loi dans l'exercice de leurs fonctions, notamment lors d'enquêtes. Ils pourront servir à obtenir un mandat ou une autorisation judiciaire.

Il faut faire la distinction entre un détenteur de compte (l'abonné) et l'utilisateur effectif du service de télécommunication. Il peut s'agir de deux individus différents. La personne qui utilise, par exemple, un poste informatique afin de commettre une infraction n'est pas nécessairement celle dont le nom est inscrit sur les factures du service Internet. À cause de cette incertitude et d'une atteinte injustifiée à la vie privée, la Cour fédérale a refusé d'ordonner la communication du nom des détenteurs des comptes Internet qui ont servi aux téléchargements de fichiers musicaux protégés par droit d'auteur(47). En vertu du projet de loi, les télécommunicateurs sont tenus de fournir, sur demande des personnes désignées, ce type de renseignement qui est associé aux abonnés.

Par ailleurs, les télécommunicateurs ne sont pas obligés de recueillir d'autres renseignements que ceux qu'ils collectent déjà dans le cours normal de leur entreprise. Le projet de loi utilise les termes « les renseignements qu'il [le télécommunicateur] a en sa possession ou à sa disposition » (par. 17(1)). De plus, ils ne sont pas contraints de vérifier l'exactitude des renseignements qu'ils recueillent.

---

(46) Par exemple, un « numéro de série électronique » identifiant de manière exclusive un certain type de dispositif sans fil.

(47) *BMG Canada Inc.* c. *John Doe*, [2004] 3 R.C.F. 241, décision confirmée par (2005) 334 N.R. 268 (C.A.F).

b. Personnes désignées

Seulement une personne désignée peut présenter une demande de renseignements en vertu du projet de loi (par. 17(1)). Elle est nommée par le commissaire de la Gendarmerie royale du Canada (GRC), le directeur du Service canadien du renseignement de sécurité (SCRS), le commissaire de la concurrence ou un chef de police (par. 17(3)).

Ceux-ci ne pourront désigner qu'un petit nombre d'employés au sein de leur organisation. Le nombre de personnes désignées est restreint à cinq pour cent des effectifs ou, dans le cas d'une organisation de cent employés et moins, à cinq personnes (par. 17(4)).

c. Tout officier de police si urgence

Face à une situation d'urgence pouvant raisonnablement entraîner des blessures corporelles graves ou des dommages matériels importants, tout policier, à la place des personnes désignées, peut faire une demande de renseignements (par. 18(1) du projet de loi)[(48)]. L'officier de police devra toutefois avertir une des personnes désignées de son organisation, et cette dernière confirmera, par écrit, la demande auprès du télécommunicateur (par. 18(3)).

d. Enquête

Une demande de renseignements ne peut se faire que dans le cadre d'une enquête par le SCRS, le Bureau de la concurrence ou un service de police conformément à la loi applicable (par. 17(2)). Les renseignements ainsi obtenus devront être utilisés uniquement à cette fin ou pour des usages connexes[(49)] (art. 19 du projet de loi).

Les demandes devant porter sur des individus précis, les personnes désignées sont donc tenues de fournir, lors de leur requête, au moins un identificateur associé à l'abonné afin d'éviter les « expéditions de pêche »[(50)].

---

(48) Il s'agit des mêmes circonstances exceptionnelles que celles prévues à l'art. 184.4 du *Code*, qui porte sur l'interception des communications.

(49) Les organismes pourront, par exemple, se servir des renseignements obtenus afin de porter des accusations criminelles.

(50) Par exemple, pour obtenir le nom d'un abonné, une personne désignée pourrait fournir une adresse IP. Voir la politique de réglementation à l'égard des autres situations possibles.

e. Réponse

D’après la politique de réglementation, le télécommunicateur devra fournir les renseignements le plus tôt possible après la réception de la demande et, au plus tard, dans :

- les deux jours ouvrables (réponse écrite);
- les 30 minutes en présence d’une situation d’urgence (réponse écrite ou verbale)

f. Confidentialité

Tout le processus entourant la demande de renseignements demeure confidentiel. Le télécommunicateur ne doit pas informer un abonné du fait qu’une personne désignée a présenté une demande ou qu’il lui a transmis des renseignements (art. 22 du projet de loi).

4. Les mesures de protection

Les dispositions relatives aux renseignements sur les abonnés tentent d’établir un équilibre entre l’augmentation des pouvoirs des organismes d’application de la loi et la protection de la vie privée des individus. Si les organismes d’application de la loi peuvent obtenir ces renseignements sans mandat, le projet de loi met toutefois en place certaines mesures de protection extrajudiciaires.

a. Registres

Chaque demande de renseignements doit pouvoir être retracée. La demande doit donc être faite par écrit (par. 17(1) du projet de loi). Les personnes désignées sont également tenues de tenir un registre qui fait notamment état des motifs appuyant chaque demande et des renseignements obtenus (par. 17(6)).

b. Vérifications internes

Le commissaire de la GRC, le directeur du SCRS, le commissaire de la concurrence ou un chef de police ont l’obligation de prendre des mesures afin de vérifier, sur une base régulière, que les demandes présentées par leur organisme sont conformes à la LMTE (par. 20(1) du projet de loi). On devra ainsi examiner, entre autres, les registres et l’utilisation qui est faite des renseignements.

Le résultat de ces vérifications fera l'objet de rapports. Ils seront établis chaque fois que le commissaire de la GRC, le directeur du SCRS, le commissaire de la concurrence ou un chef de police jugera nécessaire de le faire (par. 20(2)). Le rapport sera transmis :

- dans le cas de la GRC, au ministre et au Commissaire à la protection de la vie privée;
- dans le cas du SCRS, au ministre et au comité de surveillance des activités de renseignement de sécurité;
- dans le cas du commissaire de la concurrence, au ministre de l'Industrie et au Commissaire à la protection de la vie privée;
- dans le cas d'un chef de police, au procureur général de la province et au commissaire provincial chargé de la protection de la vie privée (par. 20(2), (3) et (7)).

c. Vérifications externes

Le Commissaire à la protection de la vie privée (et les commissaires provinciaux – en vertu de leurs pouvoirs respectifs – relativement aux organisations policières des provinces) a le pouvoir de procéder à des vérifications afin d'évaluer si la GRC ou le commissaire de la concurrence respectent les dispositions relatives aux demandes de renseignements (par. 20(4)). Le comité de surveillance des activités de renseignement de sécurité peut également procéder à ces vérifications à l'égard du SCRS (par. 20(5)).

C. Pénalités

Le projet de loi prévoit deux types de manquements à la LMTE : la violation ou l'infraction. Il établit un véritable code de procédure pénale à l'égard des violations, qui représentent, selon toute vraisemblance, des contraventions de moindre gravité. Concernant les infractions, c'est la procédure sommaire prévue au *Code* qui s'applique(51). Par contre, dans les deux cas, des accusations doivent être portées dans les deux ans du fait reproché (art. 45 et 56 du projet de loi) et le défendeur peut invoquer qu'il a pris des mesures de précaution raisonnables afin d'éviter une contravention à la loi (art. 43 et 53).

---

(51) Partie XXVII du *Code*.

Par ailleurs, le ministre peut nommer des inspecteurs et des agents verbalisateurs qui surveilleront si les télécommunicateurs respectent la LMTE (par. 32(1) et 35(1) du projet de loi). Ils possèdent le pouvoir de pénétrer dans tout lieu appartenant à un télécommunicateur afin d'y examiner les documents et les installations de télécommunication (par. 33(1) et 35(3)).

Remarquons enfin que, en ce qui concerne les obligations relatives aux renseignements sur les abonnés, le projet de loi n'indique rien sur la peine qui pourrait être imposée.

1. Infractions

Le projet de loi subdivise les infractions en trois catégories en vertu du montant de l'amende qui peut être imposée. Il est à noter qu'aucune infraction (à plus forte raison, aucune violation) n'est passible d'une peine d'emprisonnement.

Un manquement aux obligations relatives à la capacité d'interception ou la contravention d'un arrêté du ministre est passible des amendes maximales, soit 100 000 $ dans le cas d'une personne physique ou 500 000 $ dans le cas d'une société (art. 51 du projet de loi). En outre, si un télécommunicateur ne possède pas la capacité d'interception requise lors de la mise à jour de son réseau, une injonction peut être ordonnée par un tribunal afin de l'empêcher d'utiliser un appareil de transmission ou un logiciel (art. 57).

Ensuite, quiconque modifie l'équipement d'interception d'un organisme d'application de la loi, omet de fournir au ministre le rapport sur la capacité d'interception, fait une fausse déclaration ou ne respecte pas les conditions d'exemption est passible de payer une amende maximale de 25 000 $ dans le cas d'une personne physique (50 000 $ lors d'une récidive) ou 100 000 $ dans le cas d'une société (250 000 $ lors d'une récidive) (par. 52(1)).

Enfin, le fait de ne pas coopérer ou d'entraver le travail d'un inspecteur constitue une infraction pénalisée par une amende maximale de 15 000 $ (par. 52(2)).

2. Violations

C’est la gouverneure en conseil, sur recommandation du ministre, qui déterminera, par règlement, quelle contravention à la LMTE ou aux règlements constituera une violation (sous-al. 31(1)*g*)(i) et art. 34 du projet de loi). La réglementation établira également le montant maximal de l’amende qui pourra être imposée pour chaque violation. Ce montant ne pourra toutefois dépasser 50 000 $ dans le cas d’une personne physique ou 250 000 $ dans le cas d’une société (sous-al. 31(1)*g*)(ii) et art. 34).

Le projet de loi met en place les grandes lignes du régime procédural :

- S’il a des motifs raisonnables de croire qu’une violation a été commise, un agent verbalisateur dresse un procès-verbal qu’il signifie à l’auteur présumé (par. 36(1)).

- Le procès-verbal mentionne l’amende que l’agent verbalisateur a l’intention d’imposer, en prenant en compte les facteurs énoncés dans la LMTE et dans la réglementation (sous-al. 31(1)*g*)(iii), al. 36(2)*c*) et par. 36(3)). L’auteur présumé de la violation a alors trois choix :

  i. Payer l’amende. Cela met fin à la procédure (art. 37).

  ii. Contester les faits reprochés ou le montant de l’amende en présentant ses observations – dans les 30 jours ou dans le délai plus long précisé au procès-verbal – à un agent verbalisateur autre que celui qui a dressé le procès-verbal (al. 36(2)*d*) et par. 38(1)). Cet agent verbalisateur rendra sa décision selon la prépondérance des probabilités (par. 38(2)). Le montant maximal de l’amende qu’il peut imposer est limité à celui inscrit au procès-verbal. Une procédure d’appel auprès du ministre est ensuite ouverte (sous-al. 31(1)*g*)(vi) et art. 40).

  iii. Ne pas payer l’amende ni présenter de contestation. Cela équivaut à un aveu de responsabilité et il devra alors payer l’amende mentionnée au procès-verbal (al. 36(2)*e*) et art. 39).

D. Exemptions

1. Exemption totale

a. « Réseaux privés »

Le projet de loi ne s’applique pas, dans son ensemble, aux « réseaux privés » (par. 5(1) du projet de loi). C’est-à-dire les personnes qui fournissent des services de télécommunication principalement à elles-mêmes, aux membres de leur famille ou à leurs employés, et non au public.

b. Institutions déterminées

De la même façon, toute disposition du projet de loi ne s'applique pas dans le cas des :

- organismes de bienfaisance enregistrés;
- établissements d'enseignement (sauf les établissements d'enseignement postsecondaire);
- hôpitaux;
- lieux de culte;
- résidences pour retraités;
- entreprises de recherche sur les télécommunications(52);
- entreprises de radiodiffusion(53) (uniquement pour leur activité de radiodiffusion) (par. 5(1)).

2. Exemption partielle

a. Les « intermédiaires »

Les télécommunicateurs qui agissent comme « intermédiaires » – c'est-à-dire ceux qui transmettent les communications pour le compte d'autres télécommunicateurs sans modifier les communications ni authentifier les utilisateurs – ne sont pas soumis aux obligations relatives à la capacité d'interception lors d'une mise à niveau de leurs réseaux ni à celles concernant les renseignements sur les abonnés (par. 5(2) du projet de loi). Par contre, ils peuvent y être assujettis par arrêté du ministre.

b. Institutions déterminées

Mis à part l'obligation de fournir des renseignements aux organismes d'application de la loi à propos de leurs installations et leurs services de télécommunication, le projet de loi ne s'applique pas aux télécommunicateurs qui exploitent principalement :

---

(52) Par exemple, l'organisme CANARIE (http://www.canarie.ca/).

(53) Au sens du par. 2(1) de la *Loi sur la radiodiffusion*.

- un établissement d’enseignement postsecondaire;
- une bibliothèque;
- un centre communautaire;
- un restaurant;
- un hôtel ou un immeuble d’habitation (par. 5(3) du projet de loi).

c. Décret d’exemption

Sur recommandation du ministre et du ministre de l’Industrie, la gouverneure en conseil peut, par décret, exempter certaines catégories de télécommunicateurs des obligations les plus importantes du projet de loi, notamment celles relatives à la capacité d’interception lors d’une mise à niveau des réseaux ou celles concernant les renseignements sur les abonnés (par. 30(1) du projet de loi). Le décret peut imposer des conditions, et l’exemption accordée ne peut être valide que pour un maximum de deux ans (par. 30(3)).

d. Demande de suspension

Sur demande motivée d’un télécommunicateur, le ministre peut, par arrêté, suspendre, pour une période maximale de trois ans, tout ou partie des obligations relatives à la capacité d’interception lors d’une mise à niveau des réseaux (par. 14(1), (2) et (5) du projet de loi). Le ministre peut assortir la suspension des conditions qu’il estime indiquées (par. 14(5)).

e. « Petits télécommunicateurs »

Le projet de loi accorde une exemption de trois ans aux télécommunicateurs qui comptent moins de 100 000 abonnés (art. 12 du projet de loi). Pendant cette période, un tel télécommunicateur n’aura pas à se conformer aux normes de capacité d’interception exigées lors de la mise à niveau de son réseau. Il devra toutefois fournir un point de raccordement physique permettant aux organismes d’application de la loi d’intercepter les communications.

E. Entrée en vigueur

L'entrée en vigueur se fera par décret, à une seule ou plusieurs dates. Dans ce dernier cas, différentes dispositions du projet de loi entreraient en vigueur à différents moments (art. 59).

COMMENTAIRE[54]

A. Organismes d'application de la loi

Au cours des consultations, les organismes d'application de la loi appuyaient généralement les propositions sur l'accès légal. Ils sont d'avis qu'il ne doit pas y avoir, au Canada, de « zones sûres » où l'interception des communications serait impossible. Ainsi, un télécommunicateur qui ne respecterait pas l'obligation de garantir une capacité d'interception devrait être sujet à une forte amende. De plus, une demande de suspension des obligations relative à la capacité d'interception ne devrait pas être acceptée si elle est présentée cinq ans après l'entrée en vigueur de la loi.

En ce qui concerne le nom et l'adresse des abonnés, ils ne croient pas qu'il s'agit de renseignements personnels. Ils sont donc d'accord avec le fait qu'ils puissent y avoir accès sans mandat ou ordonnance judiciaire. Par contre, on aurait dû également créer une base de données nationale contentant ce genre de renseignements.

B. Industrie

Si, de façon générale, l'industrie souscrit à l'idée de permettre un accès légal efficace avec l'arrivée des changements technologiques, un doute sur la nécessité du projet de loi a été soulevé. Il y aurait absence de preuve à l'effet que des enquêtes auraient échoué en raison d'une absence de capacité technique d'interception.

La question des coûts reliés à la mise en place d'une capacité d'interception standard inquiète particulièrement les entreprises de télécommunication[55]. De plus, elles

---

(54) La plupart des renseignements qui suivent proviennent de *Mémoires sur l'accès légal* (2003). Nombre d'arguments sont repris aujourd'hui.

(55) Par exemple, les frais reliés aux « droits d'utilisation » des logiciels permettant d'activer certaines fonctions particulières.

soutiennent que la prestation de services d'accès légal aux organismes d'application de la loi – comme fournir les renseignements sur les abonnés et les assister dans les procédures d'interception – engendre des coûts permanents élevés sur le plan du personnel, de la formation et de la sécurité(56). Si une indemnisation raisonnable n'est pas offerte par le gouvernement, ces coûts devront être assumés par les consommateurs. Un groupe formé d'entreprises de télécommunication et de représentants d'organisations policières a suggéré de se servir de l'argent confisqué aux criminels afin de financer les nouvelles mesures sur l'accès légal(57).

Les entreprises s'opposent à l'établissement d'exigences techniques d'interception propres au marché canadien(58). Étant donné les différences dans l'importance des marchés, les entreprises au Canada auraient à supporter des coûts supplémentaires. Certaines associations(59) proposent donc que les entreprises ne soient tenues de respecter les exigences canadiennes qu'à partir du moment où les appareils nécessaires seraient disponibles à un coût raisonnable. Elles soutiennent aussi qu'un respect des normes internationales permettrait de remplir les obligations établies dans la réglementation canadienne. Enfin, l'industrie canadienne devrait pouvoir participer à l'élaboration des normes techniques.

Par ailleurs, la question des coûts et des normes techniques devrait être prévue par une loi plutôt que par voie réglementaire, un examen parlementaire exhaustif étant nécessaire.

À propos des renseignements sur les abonnés, on a souligné que les cybercriminels peuvent toujours utiliser de faux noms, des comptes piratés ou des ordinateurs auxquels le public a accès.

---

(56) Campbell Clark, « Ottawa demands greater wiretap access », *Globe and Mail* [Toronto], 11 octobre 2005, p. A1.

(57) Jim Bronskill, « New proposal would have criminals foot wiretap bill: Controversial law could be introduced next month », *Montreal Gazette*, 31 octobre 2005, p. A11.

(58) Les exigences techniques relatives à la capacité d'interception proposées iraient plus loin que celles prescrites dans d'autres pays. Elles engloberaient des services qui ne sont pas visés par les normes américaines (ANSI) ou européennes (ETSI) (Kirsten Embree, « Lawful Access: A Summary of the Federal Government's Recent Proposals – Part II », *Internet and E-commerce Law in Canada*, vol. 6, juin 2005, p. 34; voir aussi Tyler Hamilton, « Telecoms feel heat on wiretaps », *Toronto Star*, 22 février 2005, p. D01).

(59) L'Association canadienne des télécommunications sans fil (ACTS), l'Association canadienne des télécommunications par câble (ACTC) et l'Association canadienne de la technologie de l'information (ITAC).

C. Commissaires à la protection de la vie privée et à l'information

Les défenseurs de la vie privée ont également soulevé des doutes sur la nécessité de nouvelles règles sur l'accès légal(60). Il n'aurait pas été démontré que les lois actuelles sont insuffisantes.

Les organismes d'application de la loi possèdent déjà la possibilité d'intercepter les communications transmises par les nouvelles technologies. Par exemple, des enregistreurs de clavier peuvent capter des courriels et obtenir des mots de passe, des renifleurs de paquet peuvent balayer des messages afin de détecter des mots précis et des téléphones cellulaires sont munis de systèmes permettant de suivre un individu à la trace(61). Les obligations relatives à la capacité d'interception ouvrent d'autant plus la voie à des abus de la part des organismes d'application de la loi(62).

En contraignant les entreprises à posséder une capacité d'interception, et, dans une certaine mesure, à jouer un certain rôle dans la surveillance des communications, on atténue la frontière entre les secteurs privé et public, les télécommunicateurs devenant alors des agents de l'État. En outre, l'interception d'une communication Internet peut révéler beaucoup plus de renseignements personnels que l'écoute électronique d'une conversation téléphonique. Une approche différente serait donc essentielle. Du reste, les nouvelles mesures sur l'accès légal pourront susciter la méfiance du public à l'égard des nouvelles technologies en renforçant la croyance en une surveillance permanente du « Big Brother ».

Lorsque le nom ou l'adresse d'une personne est combiné avec un identificateur unique comme un numéro de téléphone, les règles protégeant la vie privée devraient pouvoir s'appliquer. Les lois actuelles offrant une telle protection ne devraient pas être modifiées afin d'avoir accès à ce type de renseignements sans mandat.

---

(60) Commissariat à la protection de la vie privée du Canada, « Réponse à la consultation du gouvernement sur l'accès légal » (2005).

(61) Pensons notamment au système de géolocalisation par satellite (GPS).

(62) Campbell Clark, « Privacy advocates blast Web surveillance bill », *Globe and Mail*, 16 novembre 2005, p. A6.

D. Groupes de la société civile[63]

Selon les groupes de la société civile, le document de consultation n'aurait pas démontré comment les mesures contribueraient effectivement à lutter contre le terrorisme ou le crime organisé. On souligne, à ce sujet, l'absence de statistiques à l'appui d'une nouvelle loi sur l'accès légal. À titre d'alternative aux obligations mises en place, il faudrait plutôt fournir aux organismes d'application de la loi l'expertise technique et l'équipement nécessaires afin de faire face à l'évolution du crime et des technologies.

Par ailleurs, étant donné que les exigences techniques d'interception ne s'appliqueront que lors d'une mise à niveau des réseaux, cela peut constituer un frein à l'amélioration des équipements et des services. Certains télécommunicateurs préférant ne pas mettre à jour leurs réseaux afin de ne pas être contraints de respecter les nouvelles normes.

La question des renseignements sur les abonnés pose également problème. Les organismes d'application de loi devraient toujours obtenir un mandat ou une ordonnance judiciaire pour avoir accès à ces renseignements. Les mesures de protection prévues par le projet de loi ne sont pas suffisantes[64].

E. Grand public

Encore une fois, on se demande à quel besoin urgent répondent les mesures sur l'accès légal. Les institutions fédérales responsables des consultations n'auraient pas démontré les problèmes qu'Internet a créés pour les organismes d'application de la loi.

Ensuite, les mesures de protection encadrant les demandes de renseignements sur les abonnés seraient insuffisantes. Des mesures devraient être mises en place préalablement à la divulgation des renseignements et non uniquement une fois que l'organisme d'application de la loi a effectivement obtenu l'information demandée.

On s'inquiète enfin que les nouvelles obligations entraînent, au bout du compte, une augmentation des frais pour les utilisateurs.

---

(63) « Les groupes de la société civile comprennent les groupes de défense des libertés fondamentales, les groupes communautaires, des représentants des consommateurs et des ONG [Organisations non gouvernementales] s'intéressant aux questions de la protection des renseignements personnels et de l'accès à l'information et des associations du milieu juridique » (*Mémoires sur l'accès légal* (2003), p. 3).

(64) Clark (2005).