BIBLIOTHÈQUE du PARLEMENT
LIBRARY of PARLIAMENT

RÉSUMÉ LÉGISLATIF

Projet de loi C-52 :
Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention

Publication n^{o} 40-3-C52-F
Le 30 mai 2011

Erin Shaw
Division des affaires internationales, du commerce et des finances

Dominique Valiquet
Division des affaires juridiques et législatives
Service d'information et de recherche parlementaires

Résumé législatif du projet de loi C-52

La présente publication est aussi affichée en versions HTML et PDF sur IntraParl (l'intranet parlementaire) et sur le site Web du Parlement du Canada.

Dans la version électronique, les notes de fin de document contiennent des hyperliens intégrés vers certaines des sources mentionnées.

This publication is also available in English.

Les ***résumés législatifs*** de la Bibliothèque du Parlement, ainsi que l'indique leur nom, résument des projets de loi du gouvernement étudiés par le Parlement et en exposent le contexte de façon objective et impartiale. Ils sont préparés par le Service d'information et de recherche parlementaires de la Bibliothèque, qui effectue des recherches et fournit des informations et des analyses aux parlementaires, ainsi qu'aux comités du Sénat et de la Chambre des communes et aux associations parlementaires. Les résumés législatifs sont mis à jour au besoin pour tenir compte des amendements apportés aux projets de loi au cours du processus législatif.

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.

Dans ce document, tout changement d'importance depuis la dernière publication est signalé en **caractères gras**.

Publication n^{o} 40-3-C52-F
Ottawa, Canada, Bibliothèque du Parlement (2011)

TABLE DES MATIÈRES

RÉSUMÉ LÉGISLATIF DU PROJET DE LOI C-52 : LOI SUR LES ENQUÊTES VISANT LES COMMUNICATIONS ÉLECTRONIQUES CRIMINELLES ET LEUR PRÉVENTION *

1 INTRODUCTION

Le 1er novembre 2010, l'honorable Vic Toews, ministre de la Sécurité publique (le Ministre), a présenté à la Chambre des communes le projet de loi C-52 : Loi régissant les installations de télécommunication aux fins de soutien aux enquêtes (titre abrégé : « Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention »). Il est mort au *Feuilleton* à la fin de la 40e législature, le 26 mars 2011.

Le projet de loi a trait à des aspects très précis des règles régissant l'« accès légal ». L'accès légal est une technique d'enquête employée par les organismes chargés de la sécurité nationale ou du contrôle d'application des lois qui suppose l'interception de communications privées [1] et la saisie d'information lorsque la loi l'autorise. Les règles et conditions applicables à l'accès légal sont énoncées dans un certain nombre de lois fédérales, dont le *Code criminel* (le *Code*), la *Loi sur le Service canadien de renseignement de sécurité* et la *Loi sur la défense nationale* [2].

Le projet de loi reprend bon nombre des principales dispositions de deux projets de loi antérieurs morts au *Feuilleton* : d'une part, le projet de loi C-74 : Loi sur la modernisation des techniques d'enquête, présenté pendant la 1re session de la 38e législature, en novembre 2005, et mort au *Feuilleton* le 29 novembre 2005, au moment de la dissolution de la 38e législature; d'autre part, le projet de loi C-47 : Loi sur l'assistance au contrôle d'application des lois au 21e siècle, présenté pendant la 2e session de la 40e législature, en juin 2009, qui reproduisait les principales dispositions du projet de loi C-74. Le projet de loi C-47 est mort au *Feuilleton* lorsque le Parlement a été prorogé en décembre 2009 [3].

Le projet de loi C-52 répond à une préoccupation exprimée par les organismes chargés du contrôle d'application des lois, à savoir que les nouvelles technologies, notamment les communications par Internet, nuisent souvent à l'interception légale des communications. Le projet de loi prévoit ce qui suit :

- Il oblige les télécommunicateurs à avoir les moyens d'intercepter les communications transmises par leurs réseaux, quelle que soit la technologie employée pour la transmission (art. 6 à 15).
- Il donne aux organismes chargés de la sécurité nationale ou du contrôle d'application des lois accès à des renseignements de base sur les abonnés des télécommunicateurs en vertu d'un processus administratif accéléré sans recours à un mandat ou une ordonnance judiciaires. Le projet de loi prévoit par ailleurs certaines mesures de protection (art. 16 à 23).

Le projet de loi C-52 fait partie d'une série de projets de loi présentés au cours de la 3e session de la 40e législature dans le but d'instaurer un système d'accès légal au Canada. Cette série comprend :

- Le projet de loi C-51 : Loi sur les pouvoirs d'enquête au 21e siècle, qui modernise certaines infractions dans le *Code* et la *Loi sur la concurrence* pour tenir compte des nouvelles technologies de communication et fournir de nouveaux instruments d'enquête sur les crimes informatiques aux organismes chargés du contrôle d'application des lois.
- Le projet de loi C-50 : Loi visant à améliorer l'accès aux outils d'enquête sur les crimes graves, qui modifie les dispositions du *Code* relatives à l'interception de communications privées, aux dispositifs de repérage et à l'enregistrement de numéros de téléphone [4].

Un troisième projet de loi, apparenté aux deux autres, est le projet de loi C-29 : Loi protégeant les renseignements personnels des Canadiens. Il modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* pour élargir le champ des raisons pour lesquelles les organismes chargés du contrôle d'application des lois peuvent demander à des entités privées de leur fournir des renseignements personnels sans l'autorisation des intéressés. Les modifications accroissent également le nombre d'usages et de motifs de divulgation sans autorisation des intéressés pour les organismes chargés du contrôle d'application des lois susceptibles d'obtenir un accès légal à des renseignements privés conformément au projet de loi C-52 [5].

En outre, les modifications proposées dans les projets de loi C-29 et C-52 limitent les circonstances dans lesquelles les intéressés peuvent être informés que le gouvernement a demandé ou obtenu des renseignements personnels les concernant [6].

1.1 CONTEXTE

1.1.1 CYBERCRIMINALITÉ ET CYBERSÉCURITÉ

Depuis 1995, les organismes chargés du contrôle d'application des lois réclament des mesures législatives imposant à tous les télécommunicateurs de posséder les moyens techniques de permettre aux services de police de procéder à des interceptions légales sur leurs réseaux.

À l'heure actuelle, les procédures régissant l'accès aux renseignements sur les abonnés confiés aux fournisseurs de services Internet (FSI) ralentissent, selon certains, l'accès des enquêteurs à des renseignements essentiels dans le monde numérique d'aujourd'hui, qui est à la fois très rapide et pratiquement sans frontières. Certains estiment que l'incapacité technique à isoler ou intercepter des communications en temps réel risque d'entraver la tâche des enquêteurs et des procureurs. Qui plus est, les techniques de chiffrement robustes peuvent empêcher les représentants des organismes chargés de la sécurité nationale ou du contrôle d'application des lois d'avoir accès à des renseignements à moins de pouvoir avoir accès à la clé de déchiffrement [7].

Les organismes chargés de la sécurité nationale au Canada ont fait valoir qu'il fallait modifier la loi pour qu'il soit possible d'avoir un accès fiable, rapide et sûr aux données détenues par les télécommunicateurs, y compris les renseignements sur les abonnés, et ainsi pouvoir identifier les machines en réseau qui sont à l'origine de cyberattaques perfectionnées contre des cibles stratégiques et protéger les renseignements et les réseaux importants pour le Canada [8].

1.1.2 CONSULTATIONS NATIONALES

À la suite de l'élaboration d'un cadre stratégique en 2000, des représentants de Justice Canada, d'Industrie Canada et du Solliciteur général du Canada [9] ont organisé des consultations publiques en 2002 [10]. Un résumé des résultats de ces consultations a été rendu public en 2003, et le projet de loi C-54 : Loi sur la modernisation des techniques d'enquête a été présenté en novembre 2005 [11]. Sécurité publique Canada a tenu d'autres consultations en 2007, notamment auprès de représentants du secteur des télécommunications, de groupes de défense des libertés civiques et de groupes de défense des droits des victimes. Le ministre de la Sécurité publique a ensuite présenté le projet de loi C-47 : Loi sur l'assistance au contrôle d'application des lois au 21e siècle.

Les projets de loi C-54 et C-47 sont morts au *Feuilleton*.

Pendant les consultations et depuis, le débat tourne autour de la nécessité d'une loi sur l'accès légal, du degré de protection du droit à la vie privée, ainsi que du bien-fondé et du coût de l'imposition de normes techniques d'interception aux entreprises privées [12].

1.1.3 OBLIGATIONS INTERNATIONALES

Le projet de loi C-52 représente une étape vers l'harmonisation des instruments qui permettent de lutter contre la cybercriminalité à l'échelle internationale, notamment en ce qui concerne la capacité d'interception des télécommunicateurs [13]. Le Canada a signé la *Convention sur la cybercriminalité* (la Convention) du Conseil de l'Europe en novembre 2001, ainsi que le Protocole additionnel sur les crimes haineux en juillet 2005 [14]. La Convention dispose que les États parties au traité doivent créer des infractions aux termes de leurs lois internes pour criminaliser certains usages informatiques et qu'ils doivent adopter des instruments juridiques modifiés à la lumière des nouvelles technologies, par exemple pour rendre des ordonnances de production de renseignements sur les abonnés.

La Convention n'indique pas les mécanismes précis qu'il faudrait employer pour remplir les obligations prévues, laissant le choix aux États parties. Ces derniers peuvent donc décider s'il convient de fournir un mandat judiciaire ou toute autre forme d'autorisation pour donner accès aux renseignements. De plus, les procédures pénales internes que les États parties doivent adopter en vertu de la Convention ont uniquement trait aux activités des organismes chargés du contrôle d'application des lois : la Convention n'oblige pas les États parties à créer des mécanismes procéduraux permettant l'interception de communications privées ou la divulgation de renseignements personnels aux fins plus générales de la sécurité nationale.

Enfin, la Convention dispose que les États doivent respecter toutes leurs obligations nationales et internationales en matière de protection des droits de la personne lorsqu'ils remplissent celles qui relèvent du traité [15].

2 DESCRIPTION ET ANALYSE

2.1 CAPACITÉ D'INTERCEPTION (ART. 6 À 15)

À l'heure actuelle, aucune loi canadienne ne contraint les télécommunicateurs à employer des appareils capables d'intercepter des communications. Seuls les titulaires de licences employant des fréquences radio pour des services de téléphonie classique sans fil sont tenus, depuis 1996, d'avoir du matériel permettant ce genre d'interception [16]. Les autres télécommunicateurs ne sont pas assujettis à de telles conditions.

Les télécommunicateurs peuvent légalement intercepter des communications privées dans quatre circonstances :

- si l'interception fait suite à une ordonnance judiciaire;
- si elle est raisonnablement nécessaire pour préserver la qualité et le fonctionnement d'un système informatique;
- si elle est nécessaire pour protéger un système informatique contre le piratage et les cyberattaques;
- si l'auteur des communications ou son destinataire supposé a donné son consentement express ou implicite à l'interception [17].

Pour intercepter le contenu de communications privées, les organismes chargés de la sécurité nationale ou du contrôle d'application des lois doivent obtenir une autorisation préalable, généralement sous la forme d'un mandat judiciaire [18]. Le projet de loi C-52 ne modifie pas ces exigences.

Par ailleurs, le projet de loi dispose que tous les télécommunicateurs (y compris, par exemple, les FSI) doivent posséder la capacité technique de permettre aux organismes chargés de la sécurité nationale ou du contrôle d'application des lois d'intercepter des communications par l'intermédiaire du fournisseur de services une fois obtenue l'autorisation officielle.

Dans les six mois suivant la date d'entrée en vigueur du projet de loi, les télécommunicateurs devront présenter au Ministre un rapport attestant leur capacité à remplir les exigences énoncées dans le projet de loi en matière d'interception (art. 30 et 70).

2.1.1 OBLIGATIONS DES TÉLÉCOMMUNICATEURS

2.1.1.1 CAPACITÉ D'INTERCEPTION DES TÉLÉCOMMUNICATIONS (PAR. 6(1) ET AL. 7*a*))

Aux termes du projet de loi, les télécommunicateurs doivent utiliser un appareil permettant aux organismes chargés de la sécurité nationale ou du contrôle d'application des lois d'intercepter, par exemple, les adresses de courriel et de protocole Internet d'abonnés, la date et l'heure des communications et le type de fichiers transmis (données de télécommunication)[19], ainsi que le contenu des messages (données sur le contenu).

2.1.1.2 COMMUNICATION DES RENSEIGNEMENTS DEMANDÉS (ART. 6)

Lorsqu'un organisme chargé de la sécurité nationale ou du contrôle d'application des lois a obtenu l'autorisation officielle nécessaire, le télécommunicateur doit lui fournir toutes les communications légalement interceptées (par. 6(1)). Autant que possible, le télécommunicateur doit fournir la communication interceptée sous la forme précisée par l'organisme demandeur : il peut s'agir de communications déchiffrées si le télécommunicateur possède la capacité technique de le faire. Cependant, les télécommunicateurs ne sont pas tenus d'élaborer eux-mêmes des techniques de déchiffrement particulières (par. 6(4) et 6(5)).

Le projet de loi dispose que les télécommunicateurs doivent garder secrètes les procédures et demandes d'interception (par. 6(2) et art. 23).

2.1.1.3 EXIGENCES OPÉRATIONNELLES APPLICABLES AUX TÉLÉCOMMUNICATEURS (ART. 7)

L'une des principales caractéristiques du projet de loi est l'exigence faite à tous les télécommunicateurs de disposer des capacités techniques leur permettant d'intercepter les communications transmises sur leurs réseaux, notamment :

- La capacité de séparer les communications d'une personne en particulier des communications des autres usagers, puisque, généralement, les mandats judiciaires touchent une ou plusieurs personnes précises.
- La capacité d'isoler les données permettant de déterminer la date, l'heure, la durée, le volume, la destination, l'origine, etc., d'une communication (données de télécommunication) du contenu proprement dit de la communication.
- La capacité de relier les données de télécommunication au contenu d'une communication interceptée. Cela permettra, par exemple, à un organisme chargé de la sécurité nationale ou du contrôle d'application des lois d'associer l'infraction commise à une adresse de protocole Internet.

Les télécommunicateurs doivent également avoir la capacité de permettre à plusieurs organismes chargés de la sécurité nationale ou du contrôle d'application des lois d'intercepter des communications transmises en même temps par plusieurs usagers[20].

2.1.2 CONFORMITÉ (ART. 10 ET 11)

Le projet de loi dispose que les télécommunicateurs doivent respecter les nouvelles normes techniques d'interception lorsqu'ils mettent leurs systèmes à jour. Par conséquent, tout appareil de transmission acquis ou logiciel installé après l'entrée en vigueur des articles 10 et 11 du projet de loi devra être conforme aux nouvelles normes. Autrement dit, le projet de loi n'impose pas aux fournisseurs de services de mettre leurs systèmes à jour simplement pour se conformer aux nouvelles normes. Cependant, si le commissaire de la Gendarmerie royale du Canada (GRC) ou le directeur du Service canadien du renseignement de sécurité (SCRS) le demande, le Ministre a le pouvoir d'ordonner à un télécommunicateur, avant la mise à niveau du système, d'acquérir du matériel d'interception des communications conforme aux nouvelles normes techniques (al. 14(1)*d*) et *e*)).

2.2 DEMANDES DE RENSEIGNEMENTS SUR LES ABONNÉS (ART. 16 À 23)

2.2.1 SITUATION ACTUELLE

À l'heure actuelle et dans la plupart des cas, les organisations privées ne sont tenues de communiquer des renseignements personnels sur leurs clients aux organismes chargés de la sécurité nationale ou du contrôle d'application des lois sans le consentement des intéressés que si l'organisme en question produit une autorisation judiciaire ou autre autorisation officielle lui permettant d'exiger la communication de l'information. Sinon, la divulgation de renseignements personnels n'est pas obligatoire. Dans les faits, les télécommunicateurs du Canada ont tendance à communiquer volontairement des renseignements personnels lorsque leurs ententes avec les abonnés le leur permettent et généralement dans le seul but d'atténuer un danger imminent pour la vie ou les biens [21].

Une loi récente impose cependant aux FSI de prévenir d'eux-mêmes la police s'ils ont des raisons de croire que les services qu'ils fournissent servent à transmettre de la pornographie juvénile [22].

La légalité des demandes que la police adresse aux télécommunicateurs pour qu'ils communiquent librement des renseignements sur leurs abonnés (divulgation en l'absence d'un mandat) est une question dont les tribunaux ont été saisis, car on y voit une atteinte au droit à la protection contre les fouilles, les perquisitions ou les saisies abusives aux termes de l'article 8 de la *Charte canadienne des droits et libertés*, qui protège les particuliers contre l'intrusion de l'État dans leur vie privée. La Cour suprême du Canada a statué que l'on peut raisonnablement s'attendre au respect de sa vie privée à l'égard de renseignements qui révèlent des détails intimes sur son mode de vie et ses choix personnels [23]. Les décisions judiciaires rendues sur la nécessité d'un mandat pour avoir accès aux renseignements d'abonnés portent donc généralement sur la question de savoir si l'intéressé peut raisonnablement s'attendre au respect de sa vie privée à l'égard des renseignements en question.

On ne peut affirmer clairement que, à l'heure actuelle, les particuliers peuvent raisonnablement s'attendre au respect de leur vie privée à l'égard des renseignements sur les abonnés, et la jurisprudence repose sur des cas bien précis.

Un certain nombre de tribunaux inférieurs ont statué que les abonnés ne peuvent raisonnablement s'attendre au respect de leur vie privée à l'égard de ces renseignements [24], tandis que les tribunaux sont arrivés à la conclusion inverse dans d'autres causes [25]. À la lumière d'affaires récentes, il semblerait qu'il est d'autant plus raisonnable de s'attendre au respect de sa vie privée que les renseignements sur les abonnés permettent de révéler des habitudes d'utilisation du matériel de télécommunication susceptibles d'exposer des détails intimes sur le mode de vie ou la personnalité [26].

Le projet de loi vise à clarifier les types de renseignements qui peuvent être communiqués sans mandat aux organismes chargés de la sécurité nationale ou du contrôle d'application des lois.

2.2.2 DISPOSITIONS DU PROJET DE LOI

Le projet de loi prévoit un processus permettant aux personnes désignées au sein des organismes chargés de la sécurité nationale ou du contrôle d'application des lois de demander certains renseignements sur les abonnés à un télécommunicateur et de les obtenir sans mandat ou autre autorisation légale (par. 16(1)) [27]. Le projet de loi comporte de plus certaines mesures de protection.

2.2.2.1 RENSEIGNEMENTS SUSCEPTIBLES D'ÊTRE DEMANDÉS (ART. 16)

Seuls certains types de renseignements associés aux services aux abonnés et au matériel employé peuvent être obtenus sans mandat :

- le nom;
- l'adresse;
- le numéro de téléphone;
- l'adresse de courriel;
- l'adresse de protocole Internet;
- le numéro d'identification mobile;
- le numéro de série électronique;
- l'identificateur du fournisseur de services locaux;
- le numéro d'identité internationale d'équipement mobile;
- le numéro d'identité internationale d'abonné mobile;
- le numéro de module d'identité d'abonné [28].

Le projet de loi n'exige pas que les télécommunicateurs recueillent d'autres renseignements que ceux qu'ils recueillent normalement dans le cours de leurs activités ordinaires. Il ne leur impose pas non plus de vérifier l'exactitude de ces renseignements (p. ex. l'exactitude du nom ou de l'adresse postale d'un abonné).

2.2.2.2 PERSONNES DÉSIGNÉES (ART. 16)

Seules peuvent adresser, par écrit, des demandes de renseignements sur les abonnés les personnes qui exercent des fonctions liées à la protection de la sécurité nationale ou au contrôle d'application des lois et qui sont désignées par le commissaire de la GRC, le directeur du SCRS, le commissaire de la concurrence ou le chef de leur service de police (« personnes désignées ») (par. 16(3)).

Chaque organisme peut désigner un nombre limité d'employés, soit, au maximum, 5 % de son effectif ou, s'il compte 100 employés ou moins, cinq personnes (par. 16(4)).

2.2.2.3 OBJETS DES DEMANDES DE RENSEIGNEMENTS (ART. 16 ET 19)

Les policiers désignés peuvent demander, par écrit, des renseignements ayant trait à n'importe quelle fonction policière, qu'il s'agisse de l'application de lois fédérales ou provinciales ou des lois d'un État étranger. Les personnes désignées du SCRS et du commissaire de la concurrence ne peuvent demander que des renseignements relatifs à leurs fonctions en vertu de la loi habilitante applicable (par. 16(2)).

Les renseignements ainsi obtenus ne peuvent être employés qu'aux fins prévues ci-dessus ou réservés à un usage compatible avec ces fins, à moins que l'intéressé ait fourni un consentement à portée plus large (art. 19)[29]. Les ententes de services conclues entre les télécommunicateurs et les clients, qui sont en principe des contrats d'adhésion[30], pourraient comprendre une clause de consentement permettant des usages plus larges des renseignements obtenus en vertu des dispositions du projet de loi[31].

2.2.2.4 CIRCONSTANCES EXCEPTIONNELLES : DEMANDE ADRESSÉE PAR UN OFFICIER DE POLICE (ART. 17)

Tous les policiers, qu'ils soient ou non des personnes désignées en vertu des dispositions du projet de loi, auront le pouvoir de demander aux télécommunicateurs de leur fournir des renseignements sur les abonnés dans les situations d'urgence :

- s'ils ont des motifs raisonnables de croire qu'ils ne peuvent pas, avec toute la diligence voulue, faire une demande en suivant la procédure habituelle;
- s'ils ont des motifs raisonnables de croire que les renseignements demandés sont immédiatement nécessaires pour empêcher la perpétration d'un acte illicite qui causerait des blessures corporelles graves à une personne ou des dommages importants à un bien;
- si les renseignements portent directement sur la personne soupçonnée ou sur la victime ou la personne menacée (par. 17(1))[32].

Par la suite, une personne désignée du même organisme doit fournir un compte rendu écrit de la demande au télécommunicateur (par. 17(3) et (4)).

2.2.3 VÉRIFICATIONS (ART. 20)

Les demandes de renseignements doivent être adressées par écrit, et les motifs de la demande ainsi que les renseignements obtenus doivent être consignés (art. 18).

Le commissaire de la GRC, le directeur du SCRS, le commissaire de la concurrence ou le chef d'un service de police est tenu de prendre des mesures pour vérifier régulièrement que les demandes effectuées par leurs organisations respectives sont conformes aux dispositions du projet de loi et des règlements d'application (par. 20(1)).

Si l'administrateur général de l'organisme ou le chef du service de police est d'avis que la procédure de vérification a révélé quelque chose qui devrait être porté à l'attention du ministre responsable, il doit sans délai en rendre compte et préciser les mesures qu'il propose ou qui ont été prises pour redresser la situation (par. 20(2)). Le projet de loi instaure donc une norme subjective de reddition des comptes.

Selon l'organisme, le rapport de vérification doit aussi être fourni à un organisme d'examen indépendant : le commissaire à la protection de la vie privée du Canada (dans le cas de la GRC ou du commissaire de la concurrence), le Comité de surveillance des activités de renseignement de sécurité (dans le cas du SCRS) ou le fonctionnaire provincial chargé de la protection de la vie privée (dans le cas d'un service de police provincial ou municipal). Le projet de loi ne prévoit pas que ces rapports doivent être fournis à d'autres organismes provinciaux de reddition des comptes qui assument des fonctions d'examen ou de surveillance des forces policières provinciales ou municipales (par. 20(3)).

Le commissaire à la protection de la vie privée du Canada et le Comité de surveillance des activités de renseignement de sécurité ont le pouvoir de procéder à des examens externes des demandes de renseignements sur les abonnés prévues par le projet de loi (par. 20(4) et 20(5)). Le commissaire à la protection de la vie privée doit également, chaque année, rendre compte de l'exercice des pouvoirs conférés aux fonctionnaires provinciaux en matière de vérifications externes portant sur des forces policières provinciales et municipales (par. 20(6)). À l'heure actuelle, les fonctionnaires provinciaux chargés de la protection de la vie privée n'ont pas tous le pouvoir de procéder au type de vérifications externes envisagées dans le projet de loi [33].

Le projet de loi ne prévoit pas de pouvoir spécifique autorisant la Commission des plaintes du public contre la GRC (qui peut faire enquête sur le comportement de n'importe quel agent de la GRC ou de toute autre personne assujettie à la *Loi sur la Gendarmerie royale du Canada*) à prendre connaissance de renseignements ayant trait à des vérifications internes ou externes. Actuellement, la Commission n'a pas le pouvoir d'exiger la production de renseignements ou de documents à moins qu'une audience publique ait lieu relativement à une plainte en particulier [34].

2.3 DISPOSITIONS RELATIVES À L'EXÉCUTION (ART. 33 À 38)

Le Ministre peut désigner toute personne de son choix pour vérifier le respect des dispositions du projet de loi. La personne en question a le droit de se rendre sur n'importe quel lieu appartenant à un télécommunicateur pour y examiner des documents, des renseignements et des installations de télécommunication, employer des systèmes informatiques pour faire des recherches et examiner des renseignements ou employer tout autre matériel de télécommunication se trouvant sur place. Cependant, si le lieu en question est une maison d'habitation – c'est-à-dire une structure occupée à titre de résidence permanente ou temporaire – la personne désignée doit obtenir un mandat judiciaire pour y avoir accès [35]. Elle peut, sans mandat judiciaire, photocopier ou emporter des copies de renseignements trouvés sur place et pénétrer dans des lieux privés autres qu'une maison d'habitation (immeubles de bureaux, magasins, terrains privés, etc.) pour y exercer ses pouvoirs. (art. 34, 35 et 36).

Les télécommunicateurs doivent fournir toute l'aide nécessaire durant ces visites de vérification de la conformité (par. 34(3) et art. 38).

2.3.1 VIOLATIONS ET INFRACTIONS (ART. 39 À 63)

Le projet de loi prévoit deux types de contravention : les violations et les infractions, les premières étant considérées comme moins graves que les secondes. Des amendes sont prévues dans les deux cas. Le projet de loi ne prévoit pas de peines d'emprisonnement.

C'est le gouverneur en conseil qui déterminera, par règlement, les contraventions aux dispositions du projet de loi qui constituent des violations (art. 39). Les règlements fixeront également l'amende maximale qui pourra être imposée dans chaque cas. Les amendes peuvent aller jusqu'à 50 000 $ dans le cas d'une personne physique et à 250 000 $ dans le cas d'une personne morale ou de toute autre entité (sous-al. 64(1)*p*)(ii)).

Une procédure administrative permet aux personnes auxquelles sont signifiés des procès-verbaux de violation de contester leur responsabilité en présentant des observations à la personne désignée par le Ministre (art. 43). Les décisions rendues en vertu de cette procédure peuvent faire l'objet d'un appel devant le Ministre (par. 44(1)), et la décision du Ministre dans ce cas peut faire l'objet d'un contrôle judiciaire [36].

Le mode de déclaration de culpabilité par procédure sommaire énoncé dans le *Code* s'applique aux infractions, et les amendes vont de 15 000 à 250 000 $ dans le cas d'une personne physique et de 15 000 à 500 000 $ dans le cas d'une personne morale. Le projet de loi prévoit quatre catégories d'infraction (art. 55, par. 56(1) et 56(2), art. 57) :

- Contravention aux obligations liées à la capacité d'intercepter ou à un arrêté du Ministre. Les amendes dans ce cas peuvent aller jusqu'à 100 000 $ dans le cas

d'une personne physique et jusqu'à 500 000 $ dans le cas d'une personne morale ou de toute autre entité (art. 55).

- Altération du matériel d'interception d'un organisme chargé du contrôle d'application des lois; non-présentation d'un rapport concernant la capacité d'interception; renseignements faux ou trompeurs; non-respect des conditions d'une suspension ou d'une exemption. Les amendes dans ce cas ne dépassent pas 25 000 $ dans le cas d'une personne physique (50 000 $ en cas de récidive) ou 100 000 $ dans le cas d'une personne morale ou de toute autre entité (250 000 $ en cas de récidive) (par. 56(1)).
- Non-collaboration avec une personne désignée qui vérifie la conformité aux dispositions du projet de loi ou obstruction à son travail. Les amendes dans ce cas peuvent aller jusqu'à 15 000 $ (par. 56(2)).
- Contravention aux autres dispositions du projet de loi. Les amendes dans ce cas peuvent aller jusqu'à 250 000 $[37], à moins que l'infraction soit désignée par règlement comme une violation (art. 57).

Il faut obtenir le consentement du procureur général du Canada pour intenter des poursuites relativement aux deux premières catégories d'infraction (art. 58).

2.4 Exemptions (art. 5, 13, 32 et 68 et annexes 1 et 2)

Le projet de loi s'applique à tous les télécommunicateurs exploitant des systèmes de transmission au Canada, sous réserve de certaines exemptions partielles ou complètes prévues aux annexes 1 et 2. Le gouverneur en conseil peut modifier ces annexes par règlement pour ajouter ou supprimer une catégorie de télécommunicateurs (par. 5(4)). Le projet de loi prévoit également des exemptions temporaires, de deux ou trois ans au maximum selon le cas.

2.4.1 Exemptions complètes (par. 5(1) et parties 1 et 2 de l'annexe 1)

Le projet de loi ne s'applique pas aux réseaux privés, c'est-à-dire aux personnes qui fournissent des services de télécommunication principalement destinés à elles-mêmes, à leur ménage et à leurs employés, à l'exclusion du public. Il ne s'applique pas non plus aux télécommunicateurs qui fournissent des services de télécommunication destinés principalement à la vente ou à l'achat de biens et de services autres que des services de télécommunication destinés au public. Enfin, les dispositions du projet de loi ne s'appliquent pas à la fonction principale des établissements financiers, des organismes de bienfaisance, des établissements d'enseignement (sauf les établissements d'enseignement postsecondaire), des hôpitaux, des lieux de culte, des maisons de retraite, des sociétés de recherche en télécommunication et des radiodiffuseurs.

2.4.1.1 Exemptions partielles (par. 5(2) et (3) et parties 1 et 2 de l'annexe 2)

Les établissements d'enseignement postsecondaire, les bibliothèques, les centres communautaires, les restaurants, les hôtels, les immeubles en copropriété et d'habitation sont tenus de fournir des renseignements sur leurs systèmes de

télécommunication aux organismes chargés du contrôle d'application des lois, mais ne sont pas assujettis aux autres obligations énoncées dans le projet de loi.

Les télécommunicateurs qui transmettent des communications pour le compte d'autres télécommunicateurs sans modifier ces communications ni authentifier les usagers (ce qu'on appelle des intermédiaires) ne sont pas assujettis aux obligations relatives à la capacité d'interception, à moins d'arrêté contraire du Ministre (par. 14(1) et 14(2)).

2.4.1.2 EXEMPTIONS TEMPORAIRES (ART. 13, 32 ET 69)

Le projet de loi confère au Ministre le pouvoir d'exempter les télécommunicateurs qui le demandent d'une obligation relative à la capacité d'interception. Il permet aussi au gouverneur en conseil de prendre des règlements pour exempter certaines catégories de fournisseurs d'obligations importantes, dont celles qui ont trait à la capacité d'interception et à la communication de renseignements sur les abonnés. Dans les deux cas, l'exemption peut être assujettie à des conditions et rester en vigueur pour une durée maximale de trois ans (art. 13 et 32).

Le projet de loi prévoit également une exemption de trois ans pour les fournisseurs comptant moins de 100 000 abonnés. Ces fournisseurs doivent cependant fournir un point de connexion physique permettant aux organismes chargés du contrôle d'application des lois d'intercepter des communications (art. 69).

2.5 INDEMNISATION DES TÉLÉCOMMUNICATEURS (ART. 14, 21 ET 29)

Le projet de loi prévoit trois cas d'indemnisation d'un télécommunicateur par un organisme chargé du contrôle d'application des lois ou l'organisme chargé de la sécurité nationale :

- Le Ministre a rendu un arrêté visant, par exemple, à contraindre le télécommunicateur à se conformer à des obligations supplémentaires en matière de capacité d'interception (par. 14(3)).
- Le télécommunicateur a fourni des renseignements sur les abonnés à la demande de l'organisme chargé de la sécurité nationale ou du contrôle d'application des lois (par. 21(1)).
- Le télécommunicateur a fourni un « appui spécialisé en télécommunication » à l'organisme chargé de la sécurité nationale ou du contrôle d'application des lois (par. 29(1)).

La définition de la notion d'« appui spécialisé en télécommunication » et le montant et les critères d'indemnisation seront précisés dans les règlements [38].

2.6 ENTRÉE EN VIGUEUR ET EXAMEN (ART. 67 ET 71 À 73)

Le projet de loi comprend un certain nombre de dispositions de coordination qui entreront en vigueur si le Parlement adopte également les projets de loi C-29 et C-50 (art. 71 et 72).

Le projet de loi prévoit un examen parlementaire de l'application de ses dispositions cinq ans après la date d'entrée en vigueur (art. 67).

NOTES

* Holly Porteous, analyste de la Division des affaires internationales, du commerce et des finances de la Bibliothèque du Parlement, a contribué à la production du présent résumé législatif.

1. Communément appelé « écoute téléphonique » (ou branchement clandestin).
2. *Code criminel* (le *Code*), L.R.C., 1985, ch. C-46; *Loi sur le Service canadien du renseignement de sécurité*, L.R.C., 1985, ch. 23; *Loi sur la défense nationale*, L.R.C., 1985, ch. N-5.
3. Pour plus de renseignements sur ces projets de loi, voir Dominique Valiquet, *Télécommunications et accès légal : I. La situation législative au Canada*, publication n° 05-65-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 21 février 2006.
4. Pour plus de renseignements sur ces projets de loi, voir Dominique Valiquet, *Résumé législatif du projet de loi C-50 : Loi modifiant le Code criminel (interception de communications privées et mandats et ordonnances connexes)*, publication n° 40-3-C50-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 9 novembre 2010; voir aussi Dominique Valiquet et Katherine Simonds, *Résumé législatif du projet de loi C-51 : Loi sur les pouvoirs d'enquête au 21e siècle*, publication n° 40-3-C51-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 3 février 2011.
5. Projet de loi C-29 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques, 3e session, 40e législature, par. 6(6) et 6(13); voir aussi le par. 6(12). Pour plus de renseignements sur le projet de loi C-29, voir Alysia Davies, *Résumé législatif du projet de loi C-29 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques*, publication n° 40-3-C29-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 23 juin 2010.
6. Voir le projet de loi C-52, art. 71; projet de loi C-29, art. 8. Pour plus de renseignements sur le projet de loi C-29, voir Davies (2010).
7. Voir Association canadienne des chefs de police, *Résolutions*, n° 06-2007, « Lawful Access to Encrypted Electronic Media », *Resolutions Adopted at the 102nd Annual Conference*, Calgary, août 2007, p. 26.
8. Voir le Forum des politiques publiques, *Cyber Security: Developing a Canadian Strategy*, Ottawa, 27 mars 2008; Association canadienne des chefs de police, *Resolutions* (août 2007); Holly Porteous, *Cybersécurité et renseignement de sécurité : l'approche des États-Unis*, publication n° 2010-02-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 8 février 2010; voir aussi Steven Penney, « Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age », *Revue canadienne de droit pénal*, vol. 12, 2008, p. 115. Pour une pers-

pective internationale sur des problèmes semblables dans d'autres pays, voir États-Unis, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, audience de la Sous-Commission de la criminalité, du terrorisme et de la sécurité du territoire national de la Commission des lois de la Chambre des représentants, 112e Congrès (17 février 2011) (Valerie Caproni, avocate générale, Federal Bureau of Investigation); voir aussi le Conseil de l'Europe, *Convention sur la cybercriminalité : Rapport explicatif* (STE no 185), sans date, par. 219.

9. Le ministère du Solliciteur général a pris le nom de ministère de la Sécurité publique et de la Protection civile en 2003. Le poste de solliciteur général a été officiellement aboli en 2005.

10. Voir Justice Canada, Industrie Canada et Solliciteur général du Canada, *Accès légal – Document de consultation*, Ottawa, 25 août 2002.

11. Voir Nevis Consulting Group Inc. (directeur de la rédaction), *Résumé des mémoires présentés dans le cadre de la consultation sur l'accès légal*, Justice Canada, Ottawa, 28 avril 2003.

12. Pour des exemples, voir Commissaire à la protection de la vie privée du Canada, Commissaire à l'information et la protection de la vie privée de l'Alberta, Commissaire à l'information et la protection de la vie privée de la Colombie-Britannique *et al*., « Lettre portant sur les propositions relatives à l'accès légal rédigée par les commissaires à la protection de la vie privée du Canada et les protecteurs des citoyens et destinée à Sécurité publique Canada », 9 mars 2011; « Chapitre 6 : commentaires des groupes de la société civile »; *Résumé des mémoires présentés dans le cadre de la consultation sur l'accès légal*, Justice Canada, 28 avril 2003; Association canadienne des télécommunications sans fil, « Lettre », 12 octobre 2007, p. 2; voir aussi Michael Geist, « Geist : Lawful access legislation would reshape Canada's Internet », *Toronto Star*,16 novembre 2010.

13. Pour plus de renseignements sur les lois concernant l'accès légal à l'étranger, voir Dominique Valiquet, *Télécommunications et accès légal : II. La situation législative aux États-Unis, au Royaume-Uni et en Australie*, publication no 05-66F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 28 février 2006.

14. *Convention sur la cybercriminalité*, 23 novembre 2001, STE no 185, art. 18 (entrée en vigueur le 1er juillet 2004); *Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, 28 janvier 2003, STE no 189 (entré en vigueur le 1er mars 2006).

15. *Convention sur la cybercriminalité*, par. 14(1) et (2), art. 15 et préambule; Conseil de l'Europe, *Convention sur la cybercriminalité : rapport explicatif*, art. 5, 135, 145 à 148, 182, 210 à 215, 221 à 225 et 230. Pour un survol des débats portant sur la question de l'accès légal dans d'autres pays, voir États-Unis, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, audience de la Sous-Commission de la criminalité, du terrorisme et de la sécurité du territoire national de la Commission des lois de la Chambre des représentants, 112e Congrès (17 février 2011) (Susan Landau,fellow, Radcliffe Institute for Advanced Study, Université Harvard); Declan McCullagh, « Police Want Backdoor to Web Users' Private Data », *CNET News*, 3 février 2010; Royaume-Uni, Chambre des Lords, Commission spéciale sur la Constitution, *Surveillance: Citizens and the State*, vol. I: Report, 2e rapport de session 2008-2009, HLP-18-I, 6 février 2009, p. 11 à 29; voir aussi Allemagne, Cour constitutionnelle fédérale, *Data retention unconstitutional in its present form – Judgment of 2 March 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/080*, communiqué no 11/2010, 2 mars 2010.

16. Industrie Canada impose cette exigence lorsqu'il délivre des licences d'utilisation du spectre en vertu de la *Loi sur la radiocommunication*, L.R.C. (1985), ch. R-2. Les règles actuellement applicables à l'interception sont énoncées dans les *Normes d'application*

du Solliciteur général sur l'interception licite des télécommunications (révisées en novembre 1995). Voir Kirsten Embree, « Lawful Access: A Summary of the Federal Government's Recent Proposals – Part I », *Internet and E-Commerce Law in Canada*, vol. 6, mai 2005, p. 18; voir aussi Industrie Canada, « Services de communications personnelles », *Gestion du spectre et télécommunications*; et, pour un exemple, voir Industrie Canada, « Avis n° DGRB 004 -09 – Décision concernant le renouvellement des licences de spectre dans les bandes fréquences de 24 et 38 GHz et consultation sur les droits de licences de spectre dans les bandes de fréquence de 24, 28 et 38 GHz – Annexe A : Conditions de licence », *Gestion du spectre et télécommunications*, mars 2009, par. 9.

17. *Code*, al. 184(2)*a*) et *e*). Si l'auteur ou le destinataire d'une communication travaille pour ou avec un organisme chargé du contrôle d'application des lois, un mandat judiciaire est nécessaire pour que l'interception soit légale.

18. L'interception de « communications privées » est régie par les art. 183 à 196 de la partie VI du *Code*. Le Service canadien du renseignement de sécurité peut obtenir l'autorisation judiciaire d'intercepter des communications en vertu des art. 21 à 28 de la *Loi sur le Service canadien du renseignement de sécurité*. L'interception de communications par le Centre de la sécurité des télécommunications qui ne vise pas des Canadiens ou des personnes se trouvant sur le territoire canadien est possible sur autorisation ministérielle délivrée en vertu de l'art. 273.65 de la *Loi sur la défense nationale*. Ce genre d'autorisation permet l'interception de communications privées uniquement dans le but de recueillir des « renseignements sur les moyens, les intentions ou les activités d'un étranger, d'un État étranger, d'une organisation étrangère ou d'un groupe terroriste étranger et qui portent sur les affaires internationales, la défense ou la sécurité » (art. 273.61 de la *Loi sur la défense nationale*). Le Centre de la sécurité des télécommunications peut également « fournir une assistance technique et opérationnelle aux organismes fédéraux chargés du contrôle d'application des lois et de la sécurité nationale, dans l'exercice des fonctions que la loi leur confère » (al. 273.64(1)*c*) de la *Loi sur la défense nationale*).

19. Voir la définition de « données de télécommunication » au par. 2(1) du projet de loi : il s'agit de données permettant de déterminer l'origine, le type, la direction, la date, l'heure, la durée, le volume, la destination ou la terminaison de la télécommunication produite ou reçue au moyen d'une installation de télécommunication ou le type de service utilisé. On parle aussi de données liées au trafic. Selon la politique de réglementation proposée par l'ancien projet de loi C-74, un télécommunicateur qui n'aurait pas les moyens d'intercepter des données de télécommunication en temps réel doit pouvoir au moins intercepter des données dans la seconde suivant l'interception de la communication.

20. Les règlements fixeront le nombre minimal et le nombre maximal d'interceptions simultanées que les installations de télécommunication doivent être en mesure de faciliter (al. 64(1)*h*) et *i*)). Le Ministre peut cependant ordonner à un télécommunicateur de prendre des mesures pour accroître le nombre d'interceptions simultanées au-delà du nombre maximal prévu par règlement (al. 14(1)*b*)).

21. Association canadienne de la technologie de l'information, *Customer Name and Address Consultation*, Mississauga, octobre 2007, p. 1. Pour des exemples, voir Bell Canada, *Service Internet de Bell – en vigueur le 1er octobre 2010*, clauses 13 et 17; Rogers Communications Inc., *Modalités de service de Rogers*, sans date, clauses 19 et 29.

22. *Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet*, L.C. 2011, ch. 4 (en vigueur depuis le 28 mars 2011), art. 2 à 4.

23. *R.* c. *Plant*, [1993] 3 R.C.S. 281, p. 293. Voir aussi la décision rendue récemment par la Cour suprême dans l'arrêt *R.* c. *Gomboc*, [2010] 3 R.C.S. 211.

24. *R.* v. *McNeice*, 2010 BCSC 1544 (Cour suprême de la C.-B.); *R.* v. *Brousseau*, 2010 ONSC 6753 (Cour supérieure de justice de l'Ontario) (divulgation autorisée sur accord

de l'abonné); *R.* v. *Vasic* (2009), 185 C.R.R. (2d) 286 (Cour supérieure de justice de l'Ontario) (divulgation autorisée sur accord de l'abonné); *R.* v. *Wilson*, [2009] O.J. n^{o} 1067, 10 février 2009 (Cour supérieure de justice de l'Ontario); *R.* v. *Spencer*, 2009 SKQB 341 (Cour du Banc de la Reine de la Saskatchewan); *R.* v. *Ward*, 2008 CarswellOnt 4728 (Cour de justice de l'Ontario); *R.* v. *Verge*, 2009 CarswellOnt 501 (Cour de justice de l'Ontario); *R.* v. *Trapp* (2009), 330 Sask. R. 169 (Cour provinciale de la Saskatchewan).

25. *R.* v. *Nguyen* (2004), 20 C.R. (6th) 135 (Cour suprême de la C.-B.); *R.* v. *Mahmood* (2008), 236 C.C.C. (3d) 3 (Cour supérieure de justice de l'Ontario); *R.* v. *Kwok*, [2008] O.J. 2414; (Cour de justice de l'Ontario); *R.* v. *Cuttell*, 2009 ONCJ 471, 247 C.C.C. (3d) 424 (Cour de justice de l'Ontario).

26. Voir, par exemple, *R.* c. *Gomboc*, par. 100 à 104 (selon la juge en chef McLachlin et le juge Fish).

27. La politique de réglementation énoncée dans l'ancien projet de loi C-74 prévoyait que les personnes désignées devaient au moins fournir un identificateur associé à l'abonné pour éviter les « missions exploratoires ». Par exemple, pour obtenir le nom d'un abonné, la personne désignée aurait dû fournir une adresse de protocole Internet.

28. Les renseignements relatifs à l'abonné énumérés à l'art. 18 de la *Convention sur la cybercriminalité* excluent expressément les données liées au trafic.

29. Par exemple, les organismes peuvent employer les renseignements obtenus pour porter des accusations au criminel.

30. Un contrat d'adhésion est un contrat présenté sous forme normalisée par une partie et dont les termes ne sont ni négociés ni négociables.

31. Les ententes de service actuelles de Bell et de Rogers comportent des clauses standards autorisant la divulgation des renseignements confidentiels nécessaires aux pouvoirs publics en cas de danger imminent pour la vie ou les biens si la divulgation de ces renseignements peut l'éviter ou pour satisfaire aux lois et règlements en vigueur. Les ententes de service confèrent également aux fournisseurs le droit d'exercer une surveillance ou de faire enquête sur le contenu des communications ou sur l'usage qu'un abonné fait des réseaux du fournisseur : Bell Canada (1er octobre 2010), clauses 13 et 17; Rogers Communications Inc. (s.d.), clauses 19 et 29.

32. Il s'agit des circonstances exceptionnelles prévues à l'art. 184.4 du *Code* en matière d'interception des communications.

33. Commissaire à la protection de la vie privée du Canada, Commissaire à l'information et à la protection de la vie privée de l'Alberta, Commissaire à l'information et à la protection de la vie privée de Colombie-Britannique *et al*., Lettre portant sur les propositions relatives à l'accès légal rédigée par les commissaires à la protection de la vie privée du Canada et les protecteurs des citoyens et destinée à Sécurité publique Canada, 9 mars 2011.

34. *Loi sur la Gendarmerie royale du Canada*, L.R.C. (1985), ch. R-10, art. 45.37, 45.42 et 45.43 et par. 45.45(4). La Commission des plaintes du public contre la GRC n'a pas le pouvoir de contraindre le commissaire de la GRC à fournir des renseignements ou des documents hors du cadre de la procédure d'audience publique. Pour une analyse de l'étendue des pouvoirs de la Commission, voir Commission d'enquête sur les actions des responsables canadiens relativement à l'affaire Maher Arar, *Un nouveau mécanisme d'examen des activités de la GRC en matière de sécurité nationale*, Travaux publics et Services gouvernementaux Canada, Ottawa, 2006, p. 244 à 252, 483 à 494 et 514 à 558; Groupe de travail sur la gouvernance et le changement culturel à la GRC, *Rétablir la confiance – Groupe de travail sur la gouvernance et le changement culturel à la GRC*, Ottawa, décembre 2007, p. 11 à 23; Jennifer Stoddart, commissaire à la protection de la vie privée du Canada, *Droits et réalité : augmenter la*

surveillance des programmes en matière de sécurité nationale du Canada – Mémoire présenté au Comité permanent de la sécurité publique et nationale – Révision des constatations et des recommandations issues de l'enquête interne sur les actions des responsables canadiens relativement à Abdullah Almalki, Ahmad Abou-Elmaati et Muayyed Nureddin (enquête Iacobucci) et du rapport de la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar (enquête Arar), Ottawa, 7 mai 2009. Le projet de loi C-38 : Loi modifiant la Loi sur la Gendarmerie royale du Canada et modifiant d'autres lois en conséquence, 3e session, 40e législature, mort au *Feuilleton* en mars 2011, aurait permis de créer une nouvelle Commission d'examen et de traitement des plaintes relatives à la Gendarmerie royale du Canada, dotée de pouvoirs élargis et habilitée à enquêter sur le bien-fondé des activités de la GRC (art. 8). Pour plus de renseignements, voir Lyne Casavant et Dominique Valiquet, *Résumé législatif du projet de loi C-38 : Loi modifiant la Loi sur la Gendarmerie royale du Canada et modifiant d'autres lois en conséquence*, publication no 40-3-C38-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 24 septembre 2010.

35. L'expression « maison d'habitation » est définie à l'art. 2 du *Code*.

36. *Loi sur les cours fédérales*, L.R.C. (1985), ch. F-7, art. 18.1. Il est entendu que l'art. 18.1 s'applique à l'exercice du pouvoir discrétionnaire du Ministre. Voir, par exemple *Canada c. Addison & Leyen Ltd.*, [2007] 2 R.C.S. 793.

37. Par exemple les dispositions relatives aux demandes de renseignements sur les abonnés.

38. Une récente décision de la Cour suprême éclaire la question de l'indemnisation d'un télécommunicateur au titre des coûts associés à l'exécution d'une ordonnance de communication des relevés d'appels (art. 487.012 du *Code*). La Cour a estimé que divers facteurs devaient entrer en ligne de compte, dont la portée de l'ordonnance demandée, l'importance et la viabilité économique de l'objet de l'ordonnance et l'ampleur des répercussions financières de l'ordonnance sur le télécommunicateur : *Société Télé -Mobile Co. c. Ontario*, [2008] 1 R.C.S. 305.