BIBLIOTHÈQUE du PARLEMENT
LIBRARY of PARLIAMENT

RÉSUMÉ LÉGISLATIF

Projet de loi C-30 :
Loi édictant la Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le Code criminel et d'autres lois

Publication n° 41-1-C30-F
Le 15 février 2012

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-30

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} 41-1-C30-F
Ottawa, Canada, Bibliothèque du Parlement (2012)

TABLE DES MATIÈRES

RÉSUMÉ LÉGISLATIF DU PROJET DE LOI C-30 : LOI ÉDICTANT LA LOI SUR LES ENQUÊTES VISANT LES COMMUNICATIONS ÉLECTRONIQUES CRIMINELLES ET LEUR PRÉVENTION ET MODIFIANT LE CODE CRIMINEL ET D'AUTRES LOIS

1 CONTEXTE

Le 14 février 2012, l'honorable Vic Toews, ministre de la Sécurité publique (le Ministre), a présenté à la Chambre des communes le projet de loi C-30 : Loi édictant la Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le Code criminel et d'autres lois (titre abrégé : « Loi sur la protection des enfants contre les cyberprédateurs »).

1.1 OBJET DU PROJET DE LOI

Le projet de loi C-30 traite de 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 et la saisie d'information lorsque la loi l'autorise.

Le projet de loi C-30 regroupe essentiellement les dispositions des anciens projets de loi C-50, C-51 et C-52, déposés au cours de la 3e session de la 40e législature et qui sont tous morts au *Feuilleton* avant la deuxième lecture à la Chambre des communes. La structure du projet de loi C-30 suit en fait celle de ces anciens projets de loi : la partie 1 édicte une nouvelle loi régissant les « télécommunicateurs », c'est-à-dire ceux qui fournissent des services de télécommunication (ancien projet de loi C-52); la partie 2 modifie le *Code criminel* (le *Code*) et d'autres lois relativement à l'interception de communications privées (ancien projet de loi C-50), à la modernisation de certaines infractions ainsi qu'à la création d'outils d'enquête adaptés aux délits informatiques (ancien projet de loi C-51).

En outre, le projet de loi C-30 devrait être lu en conjonction avec le projet de loi C-12, qui porte également sur l'accès légal. Le projet de loi C-12 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 *volontairement* des renseignements personnels sans l'autorisation des intéressés[1].

1.2 PRINCIPALES MODIFICATIONS APPORTÉES PAR LE PROJET DE LOI

La partie 1 du projet de loi C-30 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 crée ainsi la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention* (LECECP), qui consiste :

- À obliger 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 de la LECECP).

- À donner 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 judiciaire. Le projet de loi prévoit par ailleurs certaines mesures de protection (art. 16 à 23 de la LECECP).

La partie 2 du projet de loi vise à mettre à jour le droit criminel canadien. Plus précisément, les principales modifications du projet de loi consistent :

- à permettre la délivrance, à la fois, d'une autorisation d'interception de communications et de mandats semblables, comme un mandat de perquisition (art. 8, 10 et 12 du projet de loi);
- en ce qui concerne l'interception de communications sans autorisation judiciaire préalable, à enjoindre au gouvernement de publier un rapport annuel sur le recours à cette mesure et d'aviser les personnes qui ont fait l'objet d'une telle interception (art. 13 et 14 du projet de loi);
- à étendre l'application des infractions de propagande haineuse afin de protéger les personnes qui se différencient des autres par l'origine nationale ou la déficience mentale ou physique (art. 16 du projet de loi);
- à créer l'infraction de possession d'un virus informatique dans le but de commettre un méfait (art. 21 du projet de loi);
- à donner aux organismes d'application de la loi la possibilité d'ordonner ou d'obtenir, par voie d'ordonnance judiciaire, la préservation de preuves électroniques (art. 24 du projet de loi);
- à créer de nouvelles ordonnances judiciaires de communication pour obtenir des données relatives à la transmission de communications ou des données relatives à la localisation d'une chose ou d'une personne physique (art. 24 du projet de loi);
- à créer des mandats qui permettront d'obtenir des données de transmission en temps réel et d'activer à distance des dispositifs de localisation[2] se trouvant dans certains types de technologie (art. 28 du projet de loi);
- à moderniser les infractions de pratiques commerciales trompeuses prévues dans la *Loi sur la concurrence* (art. 35 à 37 du projet de loi);
- à modifier la *Loi sur l'entraide juridique en matière criminelle* afin que les nouvelles ordonnances de communication puissent être utilisées par les autorités canadiennes qui reçoivent des demandes d'assistance d'autres pays (art. 43 du projet de loi).

1.3 PRINCIPALES DIFFÉRENCES AVEC LES ANCIENS PROJETS DE LOI SUR L'ACCÈS LÉGAL

Il existe quelques différences entre le projet de loi C-30 et les anciens projets de loi C-50, C-51 et C-52. Entre autres, le projet de loi C-30 :

- restreint le *type de renseignements* qui pourront être obtenus sans mandat (art. 16 de la LECECP);

- précise que la demande de renseignements sur les abonnés présentée par tout policier en cas d'urgence peut être faite *oralement ou par écrit* (art. 17 de la LECECP);
- prévoit comme mesure de protection une norme *objective* de reddition de compte (part. 20(2) de la LECECP);
- ne précise pas expressément, contrairement à l'ancien projet de loi C-51, que les infractions de propagande haineuse peuvent être commises par *tout moyen de communication* et comprennent le fait de *rendre accessible* du matériel haineux (art. 5 de l'ancien projet de loi C-51);
- prévoit que la durée maximale d'un ordre de préservation est de *90 jours* dans le cas d'une infraction à une loi d'un État étranger (art. 24 du projet de loi, nouveau par. 487.012(4) du *Code*);

1.4 HISTORIQUE LÉGISLATIF ET CONSULTATIONS NATIONALES

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[3].

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[4] ont organisé des consultations publiques en 2002[5]. Un résumé des résultats de ces consultations a été rendu public en 2003[6], et un premier projet de loi sur l'accès légal a été déposé en novembre 2005 : le projet de loi C-74 (Loi sur la modernisation des techniques d'enquête).

Le ministère de la Sécurité publique du 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. En 2009, le projet de loi C-47 (Loi sur l'assistance au contrôle d'application des lois au 21e siècle), qui reprenait l'essentiel des dispositions de l'ancien projet de loi C-74, a été déposé en même temps qu'un tout nouveau projet de loi sur l'accès légal : le projet de loi C-46 (Loi sur les pouvoirs d'enquête au 21e siècle). À ces deux projets de loi – qui ont été déposés de nouveau en 2010 au cours de la session suivante sous les numéros C-51 et C-52 – est venu s'ajouter le projet de loi C-50 (Loi visant à améliorer l'accès aux outils d'enquête sur les crimes graves). Tous ces projets de loi sur l'accès légal sont morts au *Feuilleton* avant d'être adoptés.

Lors de la réunion des ministres fédéraux, provinciaux et territoriaux responsables de la justice et de la sécurité publique à Charlottetown en janvier 2012, selon le communiqué du ministère fédéral de la Sécurité publique :

> tous les ministres se sont entendus sur la nécessité de renforcer et de moderniser les capacités d'enquête des organismes d'application de la loi. Les ministres ont également exhorté le gouvernement fédéral à procéder à la promulgation des projets de loi déposés antérieurement[7].

Depuis les consultations de 2002, 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[8].

Selon certains, les procédures régissant l'accès aux renseignements sur les abonnés confiés aux fournisseurs de services Internet (FSI) ralentissent 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[9].

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[10].

1.5 OBLIGATIONS INTERNATIONALES

Le projet de loi C-30 représente une étape vers l'harmonisation des instruments qui permettent de lutter contre la cybercriminalité à l'échelle internationale, notamment en ce qui concerne les ordonnances de production et de préservation de données informatiques ainsi que la capacité d'interception des télécommunicateurs[11]. 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[12]. 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. Il semble donc que le projet de loi C-30 permettra au Canada de ratifier la Convention et son protocole additionnel. On peut toutefois se demander si le projet de loi ne va pas plus loin que ce que prescrit la Convention.

En effet, 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 ou toute autre forme d'autorisation judiciaire 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[13].

2 DESCRIPTION ET ANALYSE

2.1 PARTIE 1 (ART. 2 À 5 DU PROJET DE LOI)

La partie 1 du projet de loi crée une nouvelle loi : la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention* (LECECP).

2.1.1 CAPACITÉ D'INTERCEPTION (ART. 6 À 15 DE LA LECECP)

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[14]. 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[15].

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[16]. Le projet de loi C-30 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. 5 du projet de loi).

2.1.1.1 OBLIGATIONS IMPOSÉES AUX TÉLÉCOMMUNICATEURS LORS DE MISES À JOUR

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 de la LECECP 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 relatives à l'interception (art. 14 de la LECECP).

De plus, le projet de loi C-30 prévoit une période de transition de 18 mois durant laquelle les obligations liées à la capacité d'interception seront suspendues (art. 3 du projet de loi). Le Ministre pourra toutefois ordonner à un télécommunicateur qu'il respecte ces obligations au cours de la période de transition (art. 14 de la LECECP).

2.1.1.2 Capacité d'interception des données et du contenu des télécommunications (par. 6(1) et al. 7*a*) de la LECECP)

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 (adresses IP), la date et l'heure des communications et le type de fichiers transmis (« données de télécommunication »)[17], ainsi que le contenu des messages (données sur le contenu).

2.1.1.3 Communication confidentielle des renseignements déchiffrés (art. 6 de la LECECP)

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 de la LECECP).

2.1.1.3.1 Exigences opérationnelles des appareils (art. 7 de la LECECP)

Les nouveaux appareils des télécommunicateurs devront permettre d'intercepter les communications transmises sur leurs réseaux, en plus d'avoir, 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 (adresse IP).

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.

2.1.2 DEMANDES DE RENSEIGNEMENTS SUR LES ABONNÉS (ART. 16 À 23 DE LA LECECP)

2.1.2.1 SITUATION ACTUELLE

À l'heure actuelle et dans la plupart des cas[18], les organisations privées (comme les FSI) 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. À défaut, la divulgation de renseignements personnels n'est pas obligatoire, et l'organisation a alors le choix de divulguer *volontairement* ces renseignements. Dans les faits, les télécommunicateurs du Canada ont tendance à communiquer volontairement des renseignements personnels lorsque leurs contrats de service avec les abonnés le leur permettent et généralement dans le seul but d'atténuer un danger imminent pour la vie ou les biens[19].

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 peut y voir 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[20]. 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[21], tandis que les tribunaux sont arrivés à la conclusion inverse dans d'autres causes[22]. 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[23].

Le projet de loi C-30 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.

2.1.2.2 DISPOSITIONS DE LA LECECP

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 judiciaire (par. 16(1)). Certaines mesures de protection sont également prévues pour encadrer ce processus.

2.1.2.2.1 RENSEIGNEMENTS SUSCEPTIBLES D'ÊTRE DEMANDÉS (ART. 16 DE LA LECECP)

En vertu du projet de loi, seuls six types de renseignements concernant les abonnés de services de télécommunication peuvent être obtenus sans mandat :

- le nom;
- l'adresse;
- le numéro de téléphone;
- l'adresse de courriel;
- l'adresse de protocole Internet[24];
- l'identificateur du fournisseur de services locaux.

Le projet de loi C-30 semble donc prévoir une liste de renseignements plus limitée que celle qu'établissait l'ancien projet de loi C-52. En effet, la liste prévue par ce dernier comprenait, en plus des six types de renseignements énumérés ci-dessus, des renseignements associés à l'équipement de l'abonné : le numéro d'identification mobile; le numéro de série électronique (NSE); le numéro d'identité internationale d'équipement mobile (IIEM); le numéro d'identité internationale d'abonné mobile (IIAM); et le numéro de module d'identité d'abonné (MIA).

Une autre différence avec l'ancien projet de loi C-52 a trait au contenu de la demande écrite présentée par une personne désignée : le projet de loi C-30 prévoit expressément que, pour obtenir l'un des six types de renseignements, le policier ou l'agent du SCRS devra fournir au télécommunicateur un « renseignement identificateur ». La signification d'un « renseignement identificateur » sera définie ultérieurement par règlement (al. 64(1)*l*) de la LECECP). Par hypothèse, un policier devra fournir au télécommunicateur une adresse IP afin de pouvoir obtenir le nom et l'adresse physique de l'abonné.

En outre, 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).

2.1.2.2.2 Personnes désignées (art. 16 de la LECECP)

En général, 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)).

2.1.2.2.3 Objets des demandes de renseignements (art. 16 et 19 de la LECECP)

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'abonné ait fourni un consentement à portée plus large (art. 19)[25]. Les ententes de services conclues entre les télécommunicateurs et les clients, qui sont en principe des contrats d'adhésion[26], pourraient comprendre une clause de consentement permettant des usages plus larges des renseignements obtenus en vertu des dispositions du projet de loi[27].

2.1.2.2.4 Circonstances exceptionnelles : demande adressée par tout policier (art. 17 de la LECECP)

Tout policier, qu'il soit ou non une personne désignée en vertu des dispositions du projet de loi, a le pouvoir de demander, par écrit ou oralement, aux télécommunicateurs de lui fournir, sans mandat, des renseignements sur les abonnés dans les situations d'urgence si, à la fois :

- il a des motifs raisonnables de croire qu'il ne peut pas, avec toute la diligence voulue, faire une demande en suivant la procédure habituelle;
- il a 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;
- les renseignements portent directement sur la personne soupçonnée ou sur la victime ou la personne menacée (par. 17(1))[28].

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

2.1.2.2.5 MESURES DE PROTECTION : LES VÉRIFICATIONS (ART. 18 ET 20 DE LA LECECP)

Les demandes de renseignements doivent être adressées par écrit, et les motifs de la demande ainsi que les renseignements obtenus doivent être consignés dans un registre (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)). Ils doivent alors transmettre sans délai les conclusions de cette vérification interne au ministre compétent *dans tous les cas* (par. 20(2)). L'ancien projet de loi C-52 prévoyait plutôt une norme subjective de reddition des comptes : la personne qui avait fait procéder à la vérification interne ne devait transmettre un rapport que si *elle était d'avis* que la procédure de vérification avait révélé quelque chose qui aurait dû être porté à l'attention du ministre responsable.

Selon l'organisme, le rapport de vérification interne 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 de 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[29].

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[30].

2.1.3 EXÉCUTION ET CONTRÔLE D'APPLICATION DE LA LECECP (ART. 33 À 38 DE LA LECECP)

Le Ministre peut désigner toute personne de son choix comme « inspecteur » afin de vérifier le respect des dispositions de la LECECP. L'inspecteur 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 (art. 34 et 36).

Il 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. Si le lieu en question est une maison d'habitation – c'est-à-dire une structure occupée à titre de résidence permanente ou temporaire –, l'inspecteur doit obtenir un mandat judiciaire pour y avoir accès sans le consentement de l'occupant (art. 35). Les télécommunicateurs doivent fournir toute l'aide nécessaire durant ces visites de vérification de la conformité (par. 34(3) et art. 38).

2.1.4 VIOLATIONS ET INFRACTIONS À LA LECECP (ART. 39 À 63 DE LA LECECP)

La LECECP 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. La LECECP ne prévoit pas de peines d'emprisonnement.

C'est le gouverneur en conseil qui déterminera, par règlement, les contraventions aux dispositions de la LECECP qui constitueront 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 jusqu'à 250 000 $ dans le cas d'une personne morale ou de toute autre entité.

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[31].

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 un inspecteur 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 $[32], à moins que l'infraction soit désignée par règlement comme une violation (art. 57).

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

2.1.5 TÉLÉCOMMUNICATEURS SOUMIS À LA LECECP ET EXEMPTIONS (PAR. 5(4) DE LA LECECP)

La LECECP s'applique à tous les télécommunicateurs exploitant une installation de télécommunication 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.

2.1.5.1 EXEMPTIONS COMPLÈTES (PAR. 5(1) ET ANNEXE 1 DE LA LECECP)

La LECECP 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.

2.1.5.2 EXEMPTIONS PARTIELLES (PAR. 5(2) ET (3) ET ANNEXE 2 DE LA LECECP)

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 et de

la sécurité nationale, 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)).

2.1.5.3 EXEMPTIONS TEMPORAIRES (ART. 13 ET 32 DE LA LECECP ET ART. 4 DU PROJET DE LOI)

Premièrement, la LECECP confère au Ministre le pouvoir d'exempter les télécommunicateurs qui le demandent d'une obligation relative à la capacité d'interception (art. 13). Deuxièmement, elle permet au gouverneur en conseil de prendre des règlements pour exempter certaines catégories de télécommunicateurs d'obligations importantes, dont celles qui ont trait à la capacité d'interception et à la communication de renseignements sur les abonnés. Ces deux types d'exemption temporaire peuvent être assujettis à des conditions et rester en vigueur pour une durée maximale de trois ans et deux ans respectivement (art. 32).

Le projet de loi prévoit également une exemption de trois ans pour les télécommunicateurs 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 et de la sécurité nationale d'intercepter des communications (art. 4 du projet de loi).

2.1.6 INDEMNISATION DES TÉLÉCOMMUNICATEURS (ART. 14, 21, 29 ET 66 DE LA LECECP)

La LECECP prévoit trois cas d'indemnisation d'un télécommunicateur par un organisme chargé du contrôle d'application des lois ou 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 », le montant et les critères d'indemnisation seront précisés dans les règlements[33].

2.1.7 EXAMEN PARLEMENTAIRE DE LA LECECP (ART. 67 DE LA LECECP)

La LECECP prévoit un examen parlementaire de l'application de ses dispositions cinq ans après la date d'entrée en vigueur.

2.2 PARTIE 2 (ART. 6 À 47 DU PROJET DE LOI)

La partie 2 du projet de loi modifie le *Code criminel*, la *Loi sur la concurrence* et la *Loi sur l'entraide juridique en matière criminelle* dans le but de moderniser les infractions criminelles, les instruments juridiques et les dispositions relatives à l'interception des communications privées.

2.2.1 MODIFICATIONS AU *CODE CRIMINEL*

2.2.1.1 INTERCEPTION DES COMMUNICATIONS PRIVÉES

La partie VI du *Code* (« Atteintes à la vie privée », art. 183 et suivants) est la pièce maîtresse de la législation canadienne en matière d'écoute électronique par les organismes d'application de la loi. S'appliquant à l'interception du contenu d'une communication orale ou d'une séquence vidéo et souvent qualifiée d'intrusion élevée dans la vie privée, la partie VI établit des conditions plus strictes pour la délivrance d'une autorisation judiciaire d'intercepter des communications privées que pour l'obtention d'un mandat de perquisition ou d'une ordonnance de communication[34].

Bien que les dispositions du *Code* relatives aux saisies et aux perquisitions aient été modifiées dans les années 1980 et 1990 pour comprendre une mention expresse des ordinateurs, les dispositions de la partie VI remontent en majorité à 1974.

2.2.1.1.1 AUTORISATION D'INTERCEPTION ET MANDATS CONNEXES (ART. 8, 10, 11 ET 12 DU PROJET DE LOI)

Les forces policières ont souvent recours à l'écoute électronique en conjonction avec d'autres techniques d'enquête. Étant donné qu'une demande d'autorisation judiciaire pour intercepter des communications repose parfois sur certaines des mêmes informations que celles présentées à l'appui d'une demande de mandat – de perquisition, par exemple – ou qu'elle peut provenir de la même source, le projet de loi permet au juge d'accorder à la fois l'autorisation d'interception et le mandat désiré.

Que l'interception se fasse avec le consentement de l'une des parties à la communication (art. 184.2 du *Code*), sans le consentement des parties (art. 185 et 186 du *Code*) ou pour une période maximale de 36 heures dans le cas d'une situation d'urgence (art. 188 du *Code*), le juge pourra, en plus d'accorder l'autorisation d'interception, délivrer un mandat de perquisition, une ordonnance d'assistance ou un mandat pour l'utilisation d'un dispositif de localisation ou d'un « enregistreur de données de transmission » (art. 8, 10 et 12 du projet de loi). En dehors des situations d'urgence (c.-à-d. lorsque les art. 184.2, ou 185 et 186 s'appliquent), le juge pourra en outre délivrer un mandat général, une ordonnance de communication générale ou une ordonnance de communication spécifique pour obtenir certaines informations, comme des données informatiques ou bancaires (art. 8 et 10 du projet de loi). Dans

tous les cas, ces articles du projet de loi permettront aux policiers d'enquêter plus rapidement sur une infraction passée ou éventuelle.

Tous les documents relatifs à une demande d'autorisation d'intercepter des communications sont confidentiels; c'est pourquoi ils sont placés dans un paquet scellé par le juge (art. 187 du *Code*). L'article 11 du projet de loi précise que les documents relatifs aux demandes d'ordonnance ou de mandat connexe à l'autorisation d'interception seront traités selon les règles applicables aux documents relatifs à l'autorisation d'interception, c'est-à-dire qu'ils seront gardés secrets, généralement jusqu'au procès.

2.2.1.1.2 INTERCEPTIONS DE COMMUNICATIONS SANS AUTORISATION JUDICIAIRE (ART. 9, 13 ET 14 DU PROJET DE LOI)

À l'heure actuelle, un agent de la paix peut, aux termes de l'article 184.4 du *Code*, intercepter des communications privées sans autorisation judiciaire si les conditions suivantes sont réunies : (i) il a des motifs raisonnables de croire que l'urgence de la situation est telle qu'il ne peut obtenir une autorisation; (ii) l'interception immédiate est nécessaire afin d'empêcher la perpétration d'un *acte illicite* qui causerait des dommages sérieux à une personne ou un bien; (iii) l'une des parties à la communication est la victime ou l'auteur potentiel de *l'acte illicite*. L'expression *acte illicite* n'est pas définie ailleurs dans le *Code*.

L'article 9 du projet de loi restreint, jusqu'à un certain point, le champ d'application de l'article 184.4 en remplaçant « acte illicite » par « infraction », expression qui est définie à l'article 183 du *Code*[35]. Ainsi, l'interception de communications sans autorisation dans les circonstances exceptionnelles déterminées à l'article 184.4 ne pourra se faire qu'à l'égard des infractions énumérées à l'article 183, comme c'est d'ailleurs le cas pour la plupart des autres types d'interception prévus à la partie VI.

L'article 195 du *Code* enjoint actuellement au ministre fédéral de la Sécurité publique et aux procureurs généraux de chaque province d'établir un rapport annuel portant sur l'utilisation, par les forces de l'ordre, des autorisations de surveillance vidéo et de certaines autorisations d'intercepter des communications privées en vertu de la partie VI : les autorisations pour procéder à l'interception sans le consentement des parties à la communication (art. 185 et 186 du *Code*) et les autorisations valides pour une période maximale de 36 heures, en cas d'urgence (art. 188 du *Code*).

L'article 13 du projet de loi étend cette obligation de présenter un rapport public aux interceptions sans autorisation judiciaire faites en raison des circonstances exceptionnelles déterminées à l'article 184.4 du *Code*. Il précise également les nouveaux renseignements que devra contenir ce rapport. Cependant, d'autres types d'interception et de surveillance électronique prévus au *Code* ne seront toujours pas soumis à l'obligation faite aux gouvernements de présenter un rapport public sur leur utilisation : l'interception préventive sans autorisation judiciaire (art. 184.1), l'interception avec le consentement de l'une des parties à la communication (art. 184.2) et l'utilisation d'un dispositif de localisation (art. 492.1) ou d'un « enregistreur de numéro » (art. 492.2).

Enfin, comme pour l'interception non consensuelle autorisée par un juge (art. 185 et 186 du *Code*), l'article 14 du projet de loi prévoit que, dans le cas d'une interception sans autorisation judiciaire faite en raison des circonstances exceptionnelles précisées à l'article 184.4 du *Code*, le ministre fédéral de la Sécurité publique ou le procureur général d'une province devra aviser la personne ciblée qu'elle a fait l'objet d'une interception, et ce, généralement dans les 90 jours suivant l'interception. Sur demande présentée à un juge, ce délai pourra être porté à trois ans si l'enquête policière se poursuit (art. 196 du *Code*). Comme dans la situation actuelle, cette prolongation pourra plus facilement être obtenue si l'enquête porte sur une infraction de terrorisme ou une infraction relative au crime organisé.

2.2.1.2 Modernisation des infractions

2.2.1.2.1 Propagande haineuse (art. 15 et 16 du projet de loi)

Les infractions de propagande haineuse doivent être commises à l'égard d'un « groupe identifiable ». Concernant l'infraction d'encouragement au génocide, l'article 15 du projet de loi ajoute l'origine nationale à la définition actuelle de « groupe identifiable[36] ». L'article 16 du projet de loi, qui s'applique aux infractions d'incitation publique à la haine et de fomenter volontairement la haine, ajoute à cette définition, en plus de l'origine nationale, la déficience mentale ou physique.

2.2.1.2.2 Dispositif pour voler des services de télécommunication (art. 19 du projet de loi)

À l'heure actuelle, l'article 327 du *Code* criminalise la possession, la fabrication et la vente d'un dispositif servant à voler des services de télécommunication. L'article 19 du projet de loi ajoute essentiellement le fait d'importer ou de rendre accessible un tel dispositif. De plus, le projet de loi fait de cet acte criminel une infraction mixte, c'est-à-dire que le poursuivant aura le choix de procéder par mise en accusation ou par voie sommaire.

2.2.1.2.3 Virus informatique (art. 21 du projet de loi)

Selon les dispositions actuelles du *Code*, seules la propagation d'un virus informatique[37] ou la tentative de propagation constituent une infraction[38]. Conformément aux exigences de la *Convention sur la cybercriminalité*[39], l'article 21 du projet de loi rend illégale la possession d'un virus informatique en vue de commettre une infraction de méfait, ainsi que l'importation et la mise à disposition d'un tel virus.

2.2.1.2.4 Communications fausses, indécentes ou harcelantes (art. 22 du projet de loi)

Les dispositions actuelles du *Code* qui prévoient les infractions d'envoyer un message sous un faux nom et de transmettre de faux renseignements, des propos indécents ou des messages « harassants » (terminologie actuelle du par. 372(3) du *Code*, remplacée par « harcelants » dans le projet de loi) font mention de certaines technologies de communication, utilisées pour commettre ces infractions, comme le télégramme, la radio et le téléphone[40]. L'article 22 du projet de loi modifie ces infractions en supprimant les mentions de ces technologies de communication

particulières et, pour certaines de ces infractions, en y substituant la mention de tout moyen de télécommunication. Ainsi, des accusations pourront être déposées, peu importe le moyen de transmission ou la technologie utilisée.

Par ailleurs, le projet de loi prévoit que les infractions consistant à transmettre de faux renseignements, des propos indécents ou des messages harcelants seront désormais des infractions mixtes. Par conséquent, la peine maximale prévue pour les infractions relatives aux communications indécentes et harcelantes augmentera à deux ans d'emprisonnement, dans le cas où le poursuivant aura décidé de procéder par mise en accusation.

2.2.1.3 NOUVEAUX OUTILS D'ENQUÊTE

2.2.1.3.1 ORDRE ET ORDONNANCE DE PRÉSERVATION (ART. 24 DU PROJET DE LOI)

Les renseignements sous forme électronique peuvent être détruits ou modifiés facilement et rapidement. L'article 24 du projet de loi ajoute donc au *Code* un nouvel outil d'enquête pour conserver ce type de preuve, outil qui peut prendre l'une ou l'autre des deux formes suivantes : l'ordre ou l'ordonnance de préservation. Un ordre de préservation est donné par un agent de la paix (nouvel art. 487.012 du *Code*), tandis qu'une ordonnance de préservation est rendue par un juge, sur demande d'un agent de la paix (nouvel art. 487.013 du *Code*).

L'ordre et l'ordonnance de préservation enjoignent à une personne, par exemple un télécommunicateur, de sauvegarder des « données informatiques[41] » qui sont en « sa possession ou à sa disposition » au moment où l'ordre ou l'ordonnance est reçu. Toutefois, un télécommunicateur peut toujours préserver et communiquer *volontairement* des données à un organisme d'application de la loi, même en l'absence d'un ordre ou d'une ordonnance (nouvel art. 487.0195 du *Code*).

Ce nouvel outil d'enquête se distingue de la mesure de rétention des données, en vigueur dans certains pays[42], qui contraint les télécommunicateurs à recueillir et à conserver des données pendant une période prescrite pour tous leurs abonnés, qu'ils fassent ou non l'objet d'une enquête. À l'opposé, l'ordre et l'ordonnance de préservation ne concernent qu'une télécommunication ou une personne en particulier, dans le cadre d'une enquête policière. L'ordre et l'ordonnance de préservation pourront être donnés à un télécommunicateur uniquement s'il existe des *motifs raisonnables de soupçonner*[43] qu'une infraction a été ou sera commise (nouveaux par. 487.012(2) et 487.013(2) du *Code*). Toutefois, la personne qui est soupçonnée de l'infraction ne peut être contrainte de conserver des données par suite d'un ordre ou d'une ordonnance de préservation (nouveaux par. 487.012(3) et 487.013(5) du *Code*)[44].

L'ordre et l'ordonnance de préservation représentent des mesures temporaires, c'est-à-dire qu'ils sont généralement en vigueur assez longtemps pour permettre à l'organisme d'application de la loi d'obtenir un mandat de perquisition ou une ordonnance de communication. La durée maximale d'un ordre de préservation est de 21 jours (dans le cas d'une infraction à une loi fédérale) ou de 90 jours (dans le cas d'une infraction à une loi d'un État étranger) et l'ordre ne peut être donné qu'une

seule fois (nouveaux par. 487.012(4) et (6) du *Code*), tandis que la durée maximale d'une ordonnance de préservation est de 90 jours (nouveau par. 487.013(6) du *Code*).

La personne visée par un ordre ou une ordonnance de préservation est tenue de détruire les données informatiques qui ne seraient pas conservées dans le cadre normal de son activité commerciale, après l'expiration de l'ordre ou de l'ordonnance, ou après que les données ont été remises à l'organisme d'application de la loi par suite d'une ordonnance de communication ou d'un mandat de perquisition (nouveaux art. 487.0194 et 487.0199 du *Code*).

La contravention à un ordre ou à une ordonnance de préservation constitue une infraction punissable, dans le premier cas, d'une amende maximale de 5 000 $ (nouvel art. 487.0197 du *Code*), ou, dans le deuxième cas, d'une amende maximale de 250 000 $ et d'un emprisonnement maximal de six mois, ou de l'une de ces peines (nouvel art. 487.0198 du *Code*).

2.2.1.3.2 ORDONNANCES DE COMMUNICATION (ART. 24 DU PROJET DE LOI)

Délivrée par un juge, une ordonnance de communication est semblable à un mandat de perquisition, à la différence que c'est la personne qui possède l'information qui, sur demande, la communique, au lieu que l'organisme d'application de la loi se rende sur place pour obtenir les renseignements recherchés au moyen d'une perquisition et d'une saisie. Les organismes d'application de la loi, munis d'une ordonnance de communication, peuvent alors, par exemple, obtenir plus facilement des documents se trouvant dans un autre pays.

Le *Code* prévoit déjà une procédure pour obtenir une ordonnance de communication *générale*, c'est-à-dire une ordonnance qui s'applique, peu importe le type de renseignements qu'un organisme d'application de la loi recherche[45]. La délivrance d'une telle ordonnance est basée sur l'existence de *motifs raisonnables de croire* qu'une infraction a été commise. Le *Code* prévoit également des ordonnances de communication *spécifiques*, c'est-à-dire qui visent à obtenir certains renseignements précis : des informations bancaires ou des registres d'appels téléphoniques[46]. La délivrance des ordonnances de communication spécifiques est basée sur le critère moins exigeant des *motifs raisonnables de soupçonner*.

L'article 24 du projet de loi crée de nouvelles ordonnances de communication spécifiques – dont la délivrance est basée sur l'existence de motifs raisonnables de soupçonner qu'une infraction a été ou sera commise – permettant à un agent de la paix d'obtenir d'un télécommunicateur[47] deux types de renseignements : des « données de transmission » (nouvel art. 487.016 du *Code*) et des « données de localisation » (nouvel art. 487.017 du *Code*)[48].

Essentiellement, les « données de transmission » sont des données qui indiquent l'origine, la destination, la date, l'heure, la durée, le type et le volume d'une télécommunication (p. ex. un appel téléphonique ou une communication Internet), sans comprendre le contenu de la télécommunication[49]. En cela, la définition de « données de transmission » est semblable à la définition de « données de télécommunication », applicable à la partie 1 du projet de loi C-30 créant la LECECP. Ce type de données

est utile, par exemple, pour retracer tous les télécommunicateurs qui ont participé à la transmission de données afin d'identifier le télécommunicateur initial et ainsi déterminer l'origine d'une télécommunication (nouvel art. 487.015 du *Code*). Les « données de localisation » concernent le lieu d'une chose ou d'une personne physique.

Ces nouvelles ordonnances de communication permettent aux organismes d'application de la loi d'obtenir des données de transmission ou de localisation *historiques*, c'est-à-dire des données qui étaient déjà en possession du télécommunicateur au moment où il reçoit l'ordonnance. Pour obtenir ces types de données *en temps réel*, les organismes d'application de la loi devront être munis d'un mandat.

Une procédure de révision est prévue pour contester tout type d'ordonnance de communication, existante et nouvelle (nouvel art. 487.0193 du *Code*)[50]. La personne qui a reçu une telle ordonnance peut demander à un juge de la révoquer ou de la modifier si la communication est déraisonnable[51] ou révèle des renseignements privilégiés[52]. Comme pour l'ordonnance de préservation, la violation d'une ordonnance de communication est punissable d'une amende maximale de 250 000 $ et d'un emprisonnement maximal de six mois, ou de l'une de ces peines (nouvel art. 487.0198 du *Code*).

2.2.1.3.3 MANDAT POUR UN DISPOSITIF DE LOCALISATION (ART. 28 DU PROJET DE LOI)

À l'heure actuelle, l'article 492.1 du *Code* permet à un agent de la paix, muni d'un mandat[53], d'installer secrètement un dispositif de localisation (p. ex. un dispositif GPS) sur une chose, s'il existe des motifs raisonnables de soupçonner qu'une infraction a été ou sera commise et que des renseignements utiles à l'enquête policière, notamment sur le lieu où peut se trouver une personne, peuvent être obtenus au moyen d'un tel dispositif.

L'article 28 du projet de loi maintient ce type de mandat, mais établit une distinction entre un mandat pour installer un dispositif de localisation sur *une chose*, par exemple une automobile, afin d'en suivre les déplacements (nouveau par. 492.1(1) du *Code*) et un mandat pour installer un tel dispositif sur une *chose habituellement portée ou transportée par une personne physique* afin de déterminer sa localisation et ses mouvements, par exemple un téléphone cellulaire (nouveau par. 492.1(2) du *Code*). Le mandat pour suivre les déplacements d'une chose est basé sur le critère actuel des *motifs raisonnables de soupçonner*, tandis que le mandat pour suivre les déplacements d'une personne physique prévoit un critère plus exigeant, soit l'existence de *motifs raisonnables de croire* qu'une infraction a été ou sera commise.

En plus de permettre d'*installer* un dispositif de localisation, le projet de loi permet aux organismes d'application de la loi d'*activer à distance* de tels dispositifs se trouvant dans certains types de technologie, comme les téléphones cellulaires ou les GPS dans certaines voitures (nouveau par. 492.1(3) du *Code*).

La durée maximale d'un mandat pour un dispositif de localisation demeure 60 jours. Toutefois, cette période augmente à un an dans le cas d'une infraction de terrorisme

ou d'une infraction de criminalité organisée (nouveaux par. 492.1(5) et (6) du *Code*)[54].

2.2.1.3.4 MANDAT POUR UN ENREGISTREUR DE DONNÉES DE TRANSMISSION (ART. 28 DU PROJET DE LOI)

Actuellement, le paragraphe 492.2(1) du *Code* permet à un agent de la paix, muni d'un mandat, de placer secrètement un enregistreur de numéro sur un téléphone ou une ligne téléphonique, s'il existe des motifs raisonnables de soupçonner qu'une infraction a été ou sera commise et que des renseignements utiles à l'enquête policière pourraient être obtenus au moyen d'un tel enregistreur. Ainsi, l'organisme d'application de la loi pourra obtenir les numéros de téléphone « entrants et sortants » d'un téléphone sous écoute.

L'article 28 du projet de loi prévoit un mandat qui autorise un agent de la paix à installer et activer un enregistreur de données de transmission[55] (nouvel art. 492.2 du *Code*). Comme auparavant, un tel mandat permettra aux organismes d'application de la loi d'obtenir des données téléphoniques, mais également des données indiquant l'origine et la destination d'une communication Internet, par exemple. Les services de police pourront donc avoir accès à ces données de transmission en temps réel. Et, à l'instar du mandat pour placer un enregistreur de numéros téléphoniques, le nouveau mandat est basé sur le critère des motifs raisonnables de soupçonner. Enfin, l'article 26 du projet de loi prévoit l'utilisation d'un enregistreur de données de transmission sans mandat lors de situations d'urgence.

2.2.2 MODIFICATIONS À LA *LOI SUR LA CONCURRENCE*

2.2.2.1 ORDONNANCES DE PRÉSERVATION ET DE COMMUNICATION (ART. 31 DU PROJET DE LOI)

Les nouvelles dispositions du *Code* concernant les ordres et ordonnances de préservation de données informatiques et les ordonnances de communication de données de transmission et d'informations bancaires s'appliqueront à certaines enquêtes menées en vertu de la *Loi sur la concurrence*. Ainsi, le commissaire de la concurrence pourra se servir de ces nouveaux outils d'enquête pour obtenir des preuves en matière de pratiques commerciales trompeuses et de pratiques restrictives du commerce.

2.2.2.2 MODERNISATION DES INFRACTIONS (ART. 35 À 37 DU PROJET DE LOI)

Les articles 35 à 37 du projet de loi modernisent certaines infractions de pratiques commerciales trompeuses – par exemple donner de fausses indications sur un produit ou service et le télémarketing trompeur – en remplaçant la mention du *téléphone* comme moyen de commettre ces infractions par celle de *tout moyen de télécommunication* utilisé pour communiquer oralement.

2.2.3 MODIFICATIONS À LA *LOI SUR L'ENTRAIDE JURIDIQUE EN MATIÈRE CRIMINELLE*

La *Loi sur l'entraide juridique en matière criminelle*, adoptée en 1988, confère aux tribunaux canadiens des pouvoirs coercitifs, par exemple en matière d'assignation de témoins et de mandats de perquisition, pour obtenir au Canada, au profit d'un autre État, des preuves qui seront utilisées dans des enquêtes et des poursuites criminelles dirigées par cet autre État. Elle vise à promouvoir la collaboration entre les États en mettant en place un système d'échange de renseignements et d'éléments de preuve[56].

2.2.3.1 PERQUISITIONS PAR LE COMMISSAIRE DE LA CONCURRENCE (ART. 39 DU PROJET DE LOI)

Le projet de loi habilite le commissaire de la concurrence à exécuter des mandats de perquisition délivrés en vertu de la *Loi sur l'entraide juridique en matière criminelle*.

2.2.3.2 ORDONNANCES DE COMMUNICATION (ART. 43 DU PROJET DE LOI)

Le projet de loi prévoit que les ordonnances de communication du *Code* pour obtenir des informations bancaires, des données de transmission ou de localisation pourront être utilisées par les autorités canadiennes qui reçoivent des demandes d'assistance de leurs partenaires internationaux.

NOTES

1. *Projet de loi C-12 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques*, 1re session, 41e législature, par. 6(6) et 6(12). Pour plus de renseignements sur le projet de loi C-12, voir Dara Lithwick, *Résumé législatif du projet de loi C-12 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques*, publication no 41-1-C12-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 19 octobre 2011.
2. Selon la définition au nouveau par. 492.1(8) du *Code*, il s'agit essentiellement d'un dispositif servant à enregistrer et à transmettre en temps réel des données de localisation.
3. Voir, par exemple, Association canadienne des chefs de police, *Simplifier l'accès légal – Projet de loi C-30 – Dans l'optique de l'application de la loi*, 2012; Association canadienne des chefs de police, *Lawful Access Reform: A Position Paper Prepared for the Canadian Association of Chiefs of Police*, 2008.
4. 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.
5. Voir Justice Canada, Industrie Canada et Solliciteur général du Canada, *Accès légal – Document de consultation*, Ottawa, 25 août 2002.
6. Voir Nevis Consulting Group inc. (dir.), *Résumé des mémoires présentés dans le cadre de la consultation sur l'accès légal*, Justice Canada, Ottawa, 28 avril 2003.
7. Sécurité publique Canada, *Le Gouvernement Harper présente la Loi sur la protection des enfants contre les cyberprédateurs*, communiqué, Ottawa, 14 février 2012.

8. Pour des exemples, voir Commissaire à la protection de la vie privée du Canada, « Lettre au ministre de la Sécurité publique, Vic Toews », 26 octobre 2011; 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; Michael Geist, *How to Fix Canada's Online Surveillance Bill: A 12-Step To-Do List*, 24 février 2012; Christopher Parsons, *The Issues Surrounding Subscriber Information in Bill C-30*, 28 février 2012; Danika J. Grenier, « C-30 a 'wide open' surveillance bill, provides access to telcos' data centres: Experts », *The Wire Report*, 22 février 2012; Danika J. Grenier, « Telcos Still Concerned about Unkown Costs of Lawful Access Bill », *The Wire Report*, 21 février 2012; Tim Naumetz, « Human Rights Lawyer Warns Feds' Internet Surveillance Bill Could Lead to Massive Internet Sweep », *The Hill Times*, 22 février 2012; Philippa Lawson, *Moving Toward A Surveillance Society: Proposals to Expand 'Lawful Access' In Canada*, BC Civil Liberties Association, 2012; Commissaire à l'information et à la protection de la vie privée de l'Ontario, *Beware of 'Surveillance by Design': Standing up for Freedom and Privacy*; « 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.

9. Voir Association canadienne des chefs de police, *Resolutions*, n° 06-2007, « Lawful Access to Encrypted Electronic Media », *Resolutions Adopted at the 102nd Annual Conference*, Calgary, août 2007, p. 26.

10. 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; et le Dark Space Project, *Final Report*, Bell Canada, 2011. Pour une perspective 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 n° 185, sans date, par. 219.

11. Pour plus de renseignements sur les lois concernant l'accès légal à l'étranger, voir Christopher Parsons, *Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm, and Future Canadian Policies*, 7 février 2012.

12. *Convention sur la cybercriminalité*, 23 novembre 2001, STE n° 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 n° 189 (entré en vigueur le 1er mars 2006).

13. *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.

14. 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 no 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.

15. *Code criminel* (le *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.

16. 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*).

17. 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. Cela comprend également les « données de transmission », qui s'appliquent à la partie 2 du projet de loi C-30. La *Convention sur la cybercriminalité* utilise un terme différent : les « données liées au trafic ».

18. Une exception à cette règle générale est prévue par la *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), qui impose 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.

19. Dans près de 95 % des cas, les FSI communiqueraient volontairement les renseignements demandés par la GRC (Sarah Shmidt, « Tories stand firm on 'online spying' legislation », *Postmedia News*, 13 février 2012); voir aussi l'Association canadienne de la technologie de l'information, *Customer Name and Address Consultation*, Mississauga,

octobre 2007, p. 1. Pour des exemples d'ententes de service, 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.

20. *R.* c. *Plant*, [1993] 3 R.C.S. 281, p. 293; *R.* c. *Tessling*, [2004] 3 R.C.S. 432; *R.* c. *Gomboc*, [2010] 3 R.C.S. 211.

21. *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. no 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).

22. *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).

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

24. Les renseignements relatifs à l'abonné énumérés à l'art. 18 de la *Convention sur la cybercriminalité* excluent expressément les données liées au trafic, qui comprennent entre autres l'adresse IP (*Convention sur la cybercriminalité*, Rapport explicatif, par. 30).

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

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

27. 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.

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

29. Commissaire à la protection de la vie privée du Canada *et al.* (9 mars 2011).

30. *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.

31. *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.

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

33. 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.

34. Pour plus d'informations sur l'écoute électronique, 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 no 40-3-C50, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 9 novembre 2010.

35. Voir les infractions énumérées à l'art. 183 sous la définition d'« infraction ». Cette liste comprend aujourd'hui un grand nombre d'infractions et ne cesse de s'allonger à mesure que de nouvelles lois relatives au droit criminel ajoutent des infractions au *Code*.

36. Selon la définition actuelle qu'en donne le *Code* au par. 318(4), « groupe identifiable » désigne : « toute section du public qui se différencie des autres par la couleur, la race, la religion, l'origine ethnique ou l'orientation sexuelle ». La définition prévue à l'art. 2 du *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* comprend également l'origine nationale. Le par. 20 du Rapport explicatif du Protocole précise que : « [l]a notion "d'origine nationale", doit être interprétée dans un large sens factuel. Il peut se référer à l'histoire d'une personne, non seulement quant à la nationalité ou l'origine de ses ancêtres, mais aussi par rapport à sa propre appartenance nationale, indépendamment du fait que cette personne possède ou non cette nationalité au sens juridique du terme. Lorsqu'une personne possède plusieurs nationalités ou est apatride, l'interprétation large de cette notion permet de la protéger si elle est discriminée sur la base de l'un de ces motifs. De plus, la notion "d'origine nationale" peut non seulement se référer à l'appartenance à un Pays qui est reconnu comme tel par la communauté internationale, mais aussi aux minorités ou à tout autre groupe de personne avec des caractéristiques similaires. »

37. Le terme « virus informatique » comprend aussi, dans le présent résumé législatif, les autres dispositifs malveillants, comme les vers informatiques.

38. *Code*, par. 430(1.1). Voir aussi l'art. 342.2.

39. *Convention sur la cybercriminalité*, art. 6.

40. *Code*, art. 371 et 372.

41. La définition de « données informatiques » est donnée au par. 20(4) du projet de loi. Il s'agit essentiellement de données pouvant être traitées par ordinateur.

42. Parlement européen, *Directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE*, 15 mars 2006.

43. Le critère des *motifs raisonnables de soupçonner* est moins exigeant que le critère usuel des *motifs raisonnables de croire* qu'une infraction a été ou sera commise. Quoique plus rare, le critère des *motifs raisonnables de soupçonner* est toutefois déjà prévu par certaines autres dispositions du *Code*.

44. De la même façon, les ordonnances de communication ne peuvent contraindre le suspect d'une enquête à communiquer des renseignements (voir les nouveaux art. 487.014 à 487.018 du *Code*).

45. *Code*, art. 487.012 (voir aussi le nouvel art. 487.014, ajouté par le projet de loi, qui prévoit une ordonnance de communication générale semblable).

46. *Code*, par. 487.013(1) et (4) (voir aussi le nouvel art. 487.018, ajouté par le projet de loi) et 492.2(2).

47. L'agent de la paix peut aussi obtenir ces renseignements d'une autre personne, sauf le suspect de l'enquête policière, qui a en sa possession ou à sa disposition les données recherchées.

48. Voir les définitions de ces types de données dans le nouvel art. 487.011, ajouté par le projet de loi.

49. L'article premier de la *Convention sur la cybercriminalité* prévoit une définition semblable, mais utilise plutôt le terme « données relatives au trafic ».

50. Une procédure semblable est actuellement prévue à l'art. 487.015 du *Code*.

51. Voir la note 33.

52. L'ordonnance de communication peut être assortie de conditions afin de protéger les renseignements visés par le secret professionnel de l'avocat (nouveau par. 487.019(1) du *Code*, ajouté par le projet de loi).

53. S'il y a urgence et les conditions d'obtention du mandat sont présentes, un mandat n'est pas nécessaire. Il en est de même dans le cas d'une perquisition et de l'enregistreur de données de transmission (*Code*, art. 487.11; voir aussi l'art. 26 du projet de loi).

54. Cette augmentation de la durée correspond à la situation actuelle en matière d'écoute électronique relative aux infractions de terrorisme et de crime organisé (art. 186.1 du *Code*).

55. Voir la définition au nouveau par. 492.2(6) du *Code*.

56. Ces informations proviennent de Ministère de la Justice, *Le Service fédéral des poursuites – Guide*, partie VIII : « L'entraide internationale », chap. 43 : « L'entraide juridique en matière pénale ».