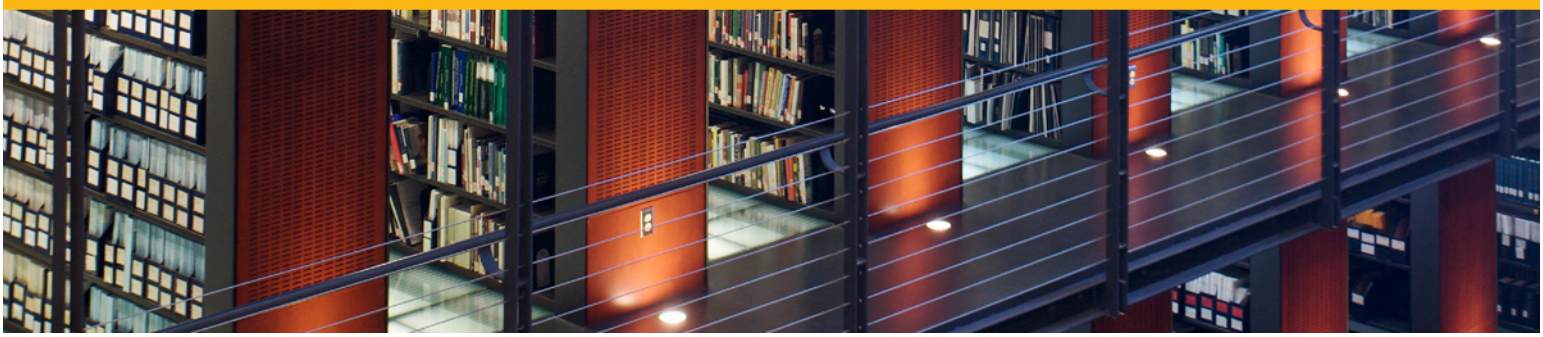
BIBLIOTHÈQUE du PARLEMENT
LIBRARY of PARLIAMENT

ÉTUDE GÉNÉRALE



Télécommunications et accès légal : la situation législative aux États-Unis, au Royaume-Uni et en Australie

Publication n^{o} 2005-66-F
Le 28 février 2006
Révisée le 6 août 2012

Rebecca Katz
Dominique Valiquet

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

Télécommunications et accès légal : la situation législative aux États-Unis, au Royaume-Uni et en Australie

(Étude générale)

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 ***études générales*** de la Bibliothèque du Parlement sont des analyses approfondies de questions stratégiques. Elles présentent notamment le contexte historique, des informations à jour et des références, et abordent souvent les questions avant même qu'elles deviennent actuelles. Les études générales sont préparées 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, et ce, de façon objective et impartiale.

Publication n^{o} 2005-66-F
Ottawa, Canada, Bibliothèque du Parlement (2012)

TABLE DES MATIÈRES

TÉLÉCOMMUNICATIONS ET ACCÈS LÉGAL : LA SITUATION LÉGISLATIVE AUX ÉTATS-UNIS, AU ROYAUME-UNI ET EN AUSTRALIE

1 INTRODUCTION

La présente étude traite de « l'accès légal [1] », une technique d'enquête à la disposition des organismes chargés de la sécurité nationale et de l'application des lois [2]. Cette technique consiste à intercepter des communications [3] et à saisir de l'information au cours d'une perquisition, lorsque la loi l'autorise.

Au cours de la première session de la 41e législature, en février 2012, le ministre de la Sécurité publique a présenté un projet de loi sur « l'écoute électronique » à l'ère des nouvelles technologies électroniques. 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 ») porte sur un sujet déjà abordé dans plusieurs autres projets de loi, notamment les projets de loi C-50, C-51 et C-52, présentés au cours de la troisième session de la 40e législature, ainsi que le projet de loi C-74, présenté durant la première session de la 38e législature.

Le projet de loi C-30 répond aux préoccupations exprimées par les organismes chargés de l'application des lois et de la sécurité nationale selon lesquelles les nouvelles technologies – comme les communications par Internet – posent souvent des obstacles à l'interception légale de communications. Le projet de loi comporte deux parties, chacune correspondant à l'un de ses principaux objectifs.

- La partie 1 crée la Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention, qui régit les fournisseurs de services de télécommunication (également appelés les télécommunicateurs).
- La partie 2 modifie le *Code criminel* et plusieurs autres lois dans le but d'actualiser les techniques d'enquête et d'interception dont disposent les organismes chargés de l'application des lois, et de mettre à jour certaines infractions.

Par ailleurs, le projet de loi C-12, déposé plusieurs mois avant le C-30, modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* pour élargir les circonstances dans lesquelles les organismes chargés de l'application des lois peuvent demander à des organismes privés de leur communiquer des renseignements personnels sans le consentement de la personne concernée.

Le débat législatif sur le projet de loi C-30 et ses prédécesseurs a surtout porté sur la protection de la vie privée. Mais d'autres facteurs importants sont pris en considération, notamment la mise en place obligatoire d'une capacité d'interception par les télécommunicateurs (y compris les fournisseurs de services Internet), le coût associé, les normes techniques à respecter et la nécessité d'introduire de nouvelles règles en matière d'accès légal. Le débat sur ces points se poursuit.

En plus de répondre aux préoccupations des autorités canadiennes chargées d'appliquer les lois, le projet de loi C-30 contribue à l'harmonisation des méthodes disponibles pour lutter contre la cybercriminalité à l'échelle internationale. Le Canada a signé, en 2001, la *Convention sur la cybercriminalité*[4] du Conseil de l'Europe et, en 2005, le *Protocole additionnel* relatif aux actes de nature raciste ou xénophobe commis par le biais de systèmes informatiques. La Convention oblige les États membres à adopter des mesures législatives pour freiner toute activité criminelle ayant recours à de nouvelles technologies et criminaliser certaines utilisations des systèmes informatiques. À l'instar de certains de ses prédécesseurs, le projet de loi C-30 permettrait au Canada de ratifier la Convention et le Protocole. Ses dispositions s'apparentent également à celles des lois de plusieurs autres pays, notamment des États-Unis, du Royaume-Uni et de l'Australie. Les États-Unis et le Royaume-Uni ont tous deux ratifié la Convention, en 2006 et en 2011, respectivement, tandis que l'Australie ne l'a pas encore signée[5].

La présente étude fait une comparaison entre le projet de loi C-30 et des lois similaires en vigueur dans ces trois pays. Elle met en évidence les principales différences et similitudes, notamment par rapport à trois questions abordées dans le projet de loi canadien : la capacité d'interception, les demandes de renseignements sur les abonnés adressées aux télécommunicateurs et la délivrance de mandats pour l'installation de dispositifs de localisation. Il est utile de faire cette comparaison, car le projet de loi C-30 est le dernier élément d'une série d'importantes initiatives canadiennes sur l'accès légal ayant proposé des dispositions similaires.

2 ÉTATS-UNIS

Le régime législatif des États-Unis est l'un des plus anciens et l'un de ceux qui sont le plus souvent modifiés. Ces nombreuses modifications s'expliquent notamment par le fait que les législateurs américains avaient à l'esprit un type particulier de technologie au moment de la mise en œuvre initiale du régime[6]. Voilà pourquoi la législation américaine comporte de nombreuses déficiences et certaines incongruités historiques.

2.1 CAPACITÉ D'INTERCEPTION

Le 25 octobre 1994, en réponse aux demandes exprimées par le Federal Bureau of Investigation (FBI), le Congrès des États-Unis adoptait la *Communications Assistance for Law Enforcement Act* (CALEA)[7]. Cette loi ne porte que sur un seul volet du projet de loi C-30, soit la capacité d'interception de communications imposée aux télécommunicateurs. À l'instar du projet de loi canadien, la CALEA ne vise pas à étendre les pouvoirs d'enquête des organismes chargés de l'application des lois. Ces derniers doivent toujours obtenir une autorisation judiciaire préalable – une ordonnance judiciaire ou toute autre autorisation légitime – avant d'intercepter des communications[8].

La Federal Communications Commission (FCC) donne alors aux télécommunicateurs jusqu'au printemps 2007 pour se conformer à la CALAE[9]. Les dispositifs requis ont été fabriqués et sont aujourd'hui utilisés par les télécommunicateurs. La FCC a toutefois accordé de nombreuses exemptions, et la mise en œuvre de la CALEA n'est toujours pas terminée.

2.1.1 DISPOSITIONS SIMILAIRES

À l'heure actuelle, aucune loi canadienne n'oblige l'ensemble des télécommunicateurs à utiliser des dispositifs permettant d'intercepter des communications. Seuls les détenteurs de permis qui utilisent des radiofréquences pour les services de téléphonie vocale sans fil sont tenus, depuis 1996, de posséder l'équipement permettant d'intercepter des communications.

Comme leurs homologues américains, pour intercepter le contenu de communications privées, les organismes canadiens chargés de l'application des lois et le Service canadien du renseignement de sécurité (SCRS) doivent obtenir l'autorisation judiciaire préalable, généralement sous forme d'un mandat judiciaire [10]. Le projet de loi C-30 ne change pas ces exigences. À l'instar de la CALEA, il oblige tous les télécommunicateurs à se doter de la capacité technique qui permettra aux organismes chargés de la sécurité nationale et de l'application des lois d'intercepter des communications transmises via leurs réseaux après avoir obtenu l'autorisation judiciaire pertinente [11].

La CALEA comporte plusieurs exigences semblables à celles énoncées dans le projet de loi C-30. Les télécommunicateurs doivent notamment pouvoir :

- intercepter et isoler une communication;
- intercepter plusieurs communications simultanément;
- isoler les données de transmission [12];
- fournir la communication interceptée et les données de transmission aux organismes chargés de l'application des lois;
- supprimer, dans la mesure du possible, toute mesure prise pour protéger une communication, par exemple, le cryptage;
- s'assurer que l'interception est exécutée en toute confidentialité [13].

De plus,

- la FCC peut exempter une catégorie de télécommunicateurs des obligations de la CALEA;
- les obligations relatives à la capacité d'interception ne s'appliquent pas aux services intermédiaires ni aux réseaux privés [14].

2.1.2 DIFFÉRENCES

2.1.2.1 EXEMPLES

Il existe également des différences entre le projet de loi C-30 et la CALEA.

- La CALEA traite plus en détail la question des dépenses engagées par les télécommunicateurs pour se conformer à la loi. Le procureur général peut rembourser aux télécommunicateurs toutes les dépenses raisonnables [15], et un fonds spécial a été constitué à cette fin [16].

- La CALEA précise clairement que le procureur général consultera le secteur des télécommunications afin de mettre en œuvre des normes techniques en matière d'interception.
- La CALEA précise que si un télécommunicateur utilise des dispositifs conformes aux normes établies par l'industrie ou par une organisation, il doit respecter les exigences en matière de capacité d'interception [17].

2.1.2.2 COMMUNICATIONS PAR INTERNET

Contrairement au projet de loi C-30, qui s'applique à toutes les technologies, la CALEA visait à l'origine à faire en sorte que les organismes chargés de l'application des lois soient en mesure d'intercepter des communications téléphoniques [18]. La CALEA précise que ses dispositions ne s'appliquent pas aux fournisseurs de services Internet (FSI) [19].

En raison des craintes suscitées par les attentats terroristes et des pressions exercées par l'administration Bush [20], la FCC a émis, en septembre 2005, une ordonnance [21] précisant que les fournisseurs de service Internet à haut débit et beaucoup d'entreprises offrant des services téléphoniques par Internet [22] seraient assujettis aux dispositions de la CALEA [23]. Ces entreprises avaient jusqu'en avril 2007 pour s'y conformer.

Tout en élargissant la portée de la CALEA, l'ordonnance reste muette sur la situation des universités, des entreprises de recherche et des petits fournisseurs de services de télécommunication. Les universités et les petites entreprises qui offrent un accès à Internet via un câble de modem, une ligne numérique d'abonné ou un réseau sans fil peuvent ainsi être assujetties aux obligations onéreuses de la CALEA. En raison de cette possibilité, certains groupes, dont l'American Council on Education, ont intenté des actions en justice [24]. Au Canada, ces fournisseurs de services sont clairement exclus de l'application du projet de loi C-30.

2.2 RENSEIGNEMENTS SUR LES ABONNÉS

Actuellement, au Canada, les entreprises privées doivent, en général, communiquer des renseignements personnels sur leurs clients aux organismes chargés de la sécurité nationale ou de l'application des lois, sans le consentement des intéressés, lorsque l'organisme en question détient une autorisation judiciaire ou toute autre autorisation légale d'exiger la communication des renseignements. En l'absence de mandat, la communication de renseignements personnels n'est pas obligatoire. Au Canada, cependant, les télécommunicateurs peuvent communiquer volontairement des renseignements personnels sur leurs clients aux organismes chargés de l'application des lois dans certaines circonstances prévues dans les ententes conclues avec les abonnés. En général, toutefois, elles le font uniquement en cas de danger imminent pour la vie ou des biens.

La légalité des demandes adressées par la police aux télécommunicateurs afin qu'ils communiquent librement des renseignements sur leurs abonnés (en l'absence d'un mandat) a été contestée devant les tribunaux pour le motif qu'il s'agissait d'une

violation du droit à la protection de la vie privée en vertu de la *Charte canadienne des droits et libertés*. La Cour suprême du Canada a jugé qu'une personne peut raisonnablement s'attendre au respect de sa vie privée à l'égard de renseignements susceptibles de révéler des détails intimes sur son mode de vie ou ses choix personnels. Cependant, la communication de renseignements personnels sur des abonnés a eu lieu dans des contextes très particuliers, et les circonstances précises dans lesquelles une personne peut raisonnablement s'attendre au respect de sa vie privée à l'égard de renseignements personnels demeurent floues. Néanmoins, la récente jurisprudence porte à croire que plus les renseignements personnels sur un abonné permettent de révéler des habitudes d'utilisation susceptibles d'exposer des détails intimes sur son mode de vie ou sa personnalité, plus cette personne peut raisonnablement s'attendre au respect de sa vie privée à l'égard de ces renseignements [25].

Puisque le projet de loi C-30 vise à clarifier les types de renseignements associés aux services et à l'équipement de l'abonné pouvant être communiqués aux organismes chargés de la sécurité nationale ou de l'application des lois, en l'absence de mandat, à des fins d'enquête, les renseignements suivants y sont inclus : le nom, l'adresse, le numéro de téléphone, l'adresse électronique, l'adresse de protocole Internet (IP) et l'identificateur du fournisseur de services locaux. L'accès à d'autres renseignements exigera toujours un mandat.

Aux États-Unis, comme dans le régime proposé dans le projet de loi C-30, certaines personnes désignées au sein du gouvernement peuvent, sans avoir obtenu au préalable un mandat ou une ordonnance judiciaire, contraindre un télécommunicateur à leur fournir des renseignements sur ses abonnés [26].

Le régime américain autorise la communication d'un plus grand nombre de renseignements que le régime proposé au Canada [27]. Aux États-Unis, il semble aussi qu'un plus grand nombre de personnes soient autorisées à rendre une ordonnance administrative à cette fin [28].

2.3 MANDATS D'INSTALLATION D'UN DISPOSITIF DE LOCALISATION

Au Canada, l'article 492.1 du *Code criminel* autorise un agent de la paix muni d'un mandat – le mandat n'étant pas obligatoire dans les situations d'urgence – à installer secrètement un « dispositif de localisation » (c.-à-d. un dispositif pouvant servir à enregistrer ou à transmettre des données de localisation en temps réel, comme un système de localisation GPS) sur une *chose* (voir l'explication ci-dessous), lorsque l'agent soupçonne qu'une infraction a été ou sera commise et que les renseignements obtenus au moyen de ce dispositif, notamment le lieu où se trouve une personne, pourraient être utiles à l'enquête.

Le projet de loi C-30 maintient ce genre de mandat tout en établissant une distinction, quant à la norme de preuve requise, entre un mandat pour l'installation d'un dispositif de localisation sur une *chose*, par exemple sur une automobile afin d'en suivre les déplacements, et un mandat pour l'installation de ce genre de dispositif sur une *chose généralement portée ou transportée par une personne*, par exemple un téléphone cellulaire afin de suivre les déplacements de la personne.

En vertu du projet de loi C-30, la norme actuelle s'applique à la délivrance d'un mandat pour suivre les déplacements d'une chose, soit l'existence de motifs raisonnables de *soupçonner* qu'une infraction a été ou sera commise, tandis qu'une norme plus rigoureuse s'applique à la délivrance d'un mandat permettant de suivre les déplacements d'une personne, soit l'existence de motifs raisonnables de *croire* qu'une infraction a été ou sera commise. En plus de permettre *l'installation* d'un dispositif de localisation, déjà permise à condition d'avoir obtenu une ordonnance judiciaire, le projet de loi permet aux organismes chargés de l'application des lois d'*activer à distance* des dispositifs de ce genre se trouvant dans certains types de technologies, comme les téléphones cellulaires ou les GPS dans certaines automobiles.

Quant à l'autre type de mandat de localisation proposé dans le projet de loi C-30, le paragraphe 492.2(1) du *Code criminel* autorise un agent de la paix muni d'un mandat à installer secrètement un *enregistreur de numéros* sur un téléphone ou une ligne téléphonique lorsqu'il soupçonne qu'une infraction a été ou sera commise et que l'information obtenue au moyen de ce genre de dispositif pourrait être utile à l'enquête. L'organisme chargé de l'application des lois pourrait ainsi obtenir les numéros de téléphone entrants et sortants d'un téléphone sous écoute.

Le projet de loi C-30 prévoit également un mandat autorisant un agent de la paix à installer et à activer un *enregistreur de données de transmission*, qui indique l'origine et la destination d'une communication Internet, par exemple [29]. Les services de police auraient ainsi accès à ces données de transmission en temps réel. Comme le mandat pour l'installation d'un enregistreur de numéros de téléphone, le nouveau mandat sera basé sur le critère de l'existence de motifs raisonnables de soupçonner qu'une infraction a été ou sera commise.

Aux États-Unis, la norme que doivent respecter les organismes chargés de l'application des lois pour obtenir une ordonnance judiciaire visant l'installation d'un enregistreur de numéros de téléphone, d'un dispositif de localisation ou d'un enregistreur de données de transmission est bien moins rigoureuse que la norme canadienne : il faut que les renseignements susceptibles d'être obtenus présentent un intérêt dans le cadre d'une enquête criminelle en cours [30].

Les modifications apportées en vertu du *Patriot Act* vont encore plus loin en créant des *roving orders* (ordonnances globales) [31]. Au lieu d'obtenir un mandat judiciaire distinct pour chaque téléphone ou dispositif qu'ils souhaitent mettre sous écoute, les agents du renseignement peuvent obtenir une ordonnance globale leur permettant de mettre sous écoute plusieurs dispositifs appartenant à une même personne. Autrement dit, ces ordonnances leur permettent de cibler une personne, plutôt qu'un téléphone ou un dispositif en particulier. Le projet de loi C-30 ne semble pas aborder cette question. Il permet toutefois à un juge d'autoriser l'interception de communications et, en même temps, de délivrer les mandats nécessaires, comme des mandats de perquisition et de localisation.

3 ROYAUME-UNI

En juillet 2000, le Royaume-Uni a adopté la *Regulation of Investigatory Powers Act* (RIPA) [32] afin de refléter l'évolution technologique au sein du secteur des télécommunications. Comme le projet de loi C-30, la RIPA s'applique à toute technologie, actuelle et future.

Cette loi vise à établir un équilibre entre les pouvoirs d'enquête des organismes chargés de l'application des lois et la protection des droits fondamentaux, en particulier la protection de la vie privée [33]. C'est le ministre de l'Intérieur (Secretary of State for the Home Department, responsable des affaires intérieures) ou, dans les situations d'urgence, un haut fonctionnaire, qui délivre les mandats d'interception de communications [34].

3.1 CAPACITÉ D'INTERCEPTION

Les articles 12 à 14 de la RIPA portent sur la capacité technique d'interception des communications. La première version de ces dispositions de la RIPA a suscité la plus vive réaction de la part des télécommunicateurs, notamment par rapport aux coûts de mise en œuvre [35]. Après avoir analysé les commentaires exprimés pendant la ronde de consultations, le gouvernement est arrivé à la conclusion qu'il devait se garder d'imposer des exigences excessives, qui pourraient constituer un obstacle important au commerce. Par ailleurs, le commissaire à la protection des données (Data Protection Commissioner) a fait remarquer que les obligations imposées par le gouvernement ne devaient pas contraindre les télécommunicateurs à mettre en péril le droit de leurs clients au respect de leur vie privée [36].

3.1.1 DISPOSITIONS SIMILAIRES

Certaines dispositions de la RIPA sont similaires à celles du projet de loi C-30.

- Les fournisseurs de services de communication publics peuvent être obligés de maintenir une capacité d'interception raisonnable [37].
- Une injonction peut être adressée à un fournisseur de services de communication publics qui ne respecte pas les exigences [38].

3.1.2 DIFFÉRENCES

Il existe de nombreuses différences entre la RIPA et le projet de loi C-30. Par exemple :

- la RIPA régit les services postaux et les services de télécommunication, tandis que les dispositions du projet de loi C-30 ne s'appliquent qu'aux services de télécommunication;
- toute ordonnance délivrée par le ministre de l'Intérieur imposant une capacité d'interception doit être présentée au Parlement et approuvée par les deux chambres;
- un fournisseur de services de communication publics peut contester devant une commission consultative spécialisée l'obligation de se doter d'une capacité d'interception [39];
- le ministre de l'Intérieur peut, dans tous les cas, acquitter les frais des fournisseurs de services de communication publics [40];
- la RIPA établit un cadre pour les communications cryptées qui permet à un organisme chargé de l'application des lois muni d'une autorisation judiciaire

d'obliger *toute personne* à lui transmettre des renseignements dans un format intelligible ou à lui fournir la clé donnant accès à l'information protégée [41].

Le cadre établi dans la RIPA est plus détaillé que le régime correspondant prévu au projet de loi C-30, qui oblige les télécommunicateurs à fournir des communications décryptées seulement s'ils possèdent la capacité technique de le faire, sans toutefois les obliger à se doter de cette capacité.

3.2 RENSEIGNEMENTS SUR LES ABONNÉS

3.2.1 STOCKAGE DES DONNÉES DE TRANSMISSION

Contrairement au Canada, le Royaume-Uni s'est doté d'un système qui permet aux fournisseurs de services de communication publics de recueillir et de conserver systématiquement les données de transmission [42]. Le projet de loi C-30 ne prévoit pas de mesure semblable.

Au Royaume-Uni, les données de transmission sont également appelées « données des communications ». Ces termes désignent une vaste gamme de renseignements pouvant être conservés durant des périodes déterminées en vertu de la loi britannique. Par exemple,

- les renseignements sur un abonné [43] peuvent être conservés pendant 12 mois;
- les données téléphoniques [44] peuvent être conservées pendant 12 mois;
- les données sur les courriels envoyés et reçus [45] peuvent être conservées pendant six mois;
- les données sur les activités sur Internet [46] peuvent être conservées pendant quatre jours [47].

3.2.2 COMPARAISON AVEC LA DEMANDE DE RENSEIGNEMENTS PRÉVUE AU PROJET DE LOI C-30

Les articles 21 à 25 de la RIPA établissent un système permettant aux organismes chargés de l'application des lois d'avoir accès à des données de transmission. Ce système se compare à la demande de renseignements sur les abonnés prévue au projet de loi C-30.

Voici quelques similitudes :

- La demande est présentée par une personne désignée qui n'a pas besoin d'obtenir l'autorisation d'un juge [48].
- Il doit être possible de retracer chaque demande [49].

En revanche, il existe de grandes différences quant à la nature des renseignements. Le système britannique vise une gamme beaucoup plus vaste de renseignements (données de transmission) [50] que le projet de loi C-30 (qui ne porte que sur les

renseignements permettant d'identifier un abonné, dont son nom, son adresse et son numéro de téléphone). D'autres différences sont à signaler :

- La RIPA prévoit un critère de proportionnalité entre les renseignements demandés et le motif de la demande, et les motifs semblent être plus nombreux que ceux autorisés par le projet de loi C-30 [51].
- La législation prévoit des mesures de protection plus précises. En vertu de la RIPA, un commissaire à l'interception des communications est chargé de surveiller l'exercice des pouvoirs délégués à des personnes désignées. En outre, un tribunal est chargé d'entendre les plaintes déposées par le public [52].

3.2.3 MODIFICATIONS PROPOSÉES

En juin 2012, le ministre de l'Intérieur du Royaume-Uni a présenté au Parlement un avant-projet de loi sur les données des communications [53]. Il a fait observer que cet avant-projet serait étudié par un comité parlementaire mixte ainsi que par le comité du renseignement et de la sécurité avant d'être présenté au Parlement plus tard au cours de la session [54]. L'avant-projet de loi prévoit plusieurs modifications à la législation britannique sur l'accès légal. Il vise notamment :

- à modifier le cadre de compilation de « données sur les transmissions, l'utilisation et les abonnés [55] » pour faire en sorte que les fournisseurs de services postaux et de services de télécommunication mettent à la disposition des autorités publiques un éventail plus large de données, y compris des données que les fournisseurs de services ne produisent habituellement pas dans le cadre de leurs activités courantes;
- à mettre à jour le régime afin de permettre aux autorités publiques concernées d'obtenir les données de communications et établir une procédure permettant aux hauts fonctionnaires désignés d'avoir accès à des données, conformément aux critères fondés sur la nécessité et la proportionnalité;
- à conférer d'autres fonctions d'examen approfondi au commissaire à l'interception de communications et au tribunal d'enquête (Investigatory Powers Tribunal);
- à établir une procédure de délivrance d'ordonnances et d'indemnisation des fournisseurs de services au regard des dépenses engagées pour se conformer à la loi.

À l'instar du régime législatif en place, l'avant-projet de loi s'appliquerait aux services postaux et aux services de télécommunication. Il maintiendrait l'obligation d'obtenir une autorisation judiciaire pour avoir accès au *contenu* des communications. Il autorise uniquement l'accès à des « données sur les transmissions, l'utilisation et les abonnés », et cet accès n'exigerait pas l'autorisation d'un magistrat dans le cas des demandes faites par les forces policières et toute autre autorité publique [56].

3.3 MANDATS POUR L'INSTALLATION DE DISPOSITIFS DE LOCALISATION

Au Royaume-Uni, le ministre de l'Intérieur et d'autres personnes désignées ont le pouvoir d'autoriser l'utilisation de dispositifs de surveillance pour des motifs plus larges que ceux permis par la loi canadienne. Tant au Canada qu'au Royaume-Uni,

la prévention et la détection d'actes criminels sont considérées comme des motifs légitimes. Le Royaume-Uni reconnaît également un autre motif : le calcul et la perception des taxes, droits ou autres impôts, contributions ou charges payables à un ministère du gouvernement [57].

Par ailleurs, la loi britannique comprend une autre disposition que l'on ne trouve pas explicitement dans le projet de loi C-30 : « que la surveillance autorisée soit proportionnelle au but visé par l'exercice de cette surveillance (le critère de l'équilibre) [58] ».

4 AUSTRALIE

Le cadre du régime australien d'accès légal est défini dans deux lois principales : la *Telecommunications (Interception and Access) Act 1979* et la *Telecommunications Act 1997*. Ces deux lois obligent les organismes chargés de l'application des lois à obtenir un mandat pour accéder à des données stockées ou intercepter des communications privées en temps réel [59].

L'Australie n'a pas encore signé la *Convention sur la cybercriminalité*, contrairement au Canada, aux États-Unis et au Royaume-Uni.

4.1 CAPACITÉ D'INTERCEPTION

Les exigences relatives à la capacité d'interception sont énoncées dans la *Telecommunications Act 1997* (TA1997). C'est l'organisme australien responsable des communications et des médias, l'ACMA (Australian Communications and Media Authority), qui est chargé de contrôler le respect de ces exigences.

4.1.1 DISPOSITIONS SIMILAIRES

La TA1997 et le projet de loi C-30 présentent certaines similitudes, notamment :

- Les télécommunicateurs doivent respecter les exigences relatives à la capacité d'interception.
- Les télécommunicateurs doivent aider les organismes chargés de l'application des lois, principalement dans l'exécution des mandats et la communication de renseignements.
- Le processus doit demeurer confidentiel. Aucun télécommunicateur ne peut divulguer des renseignements interceptés, et les renseignements personnels des utilisateurs sont protégés en vertu des dispositions régissant les données de transmission, le contenu des communications et les renseignements personnels.
- Des exemptions peuvent être accordées [60].

4.1.2 DIFFÉRENCES

Il existe également des différences entre la TA1997 australienne et le projet de loi C-30.

- Tous les télécommunicateurs doivent présenter un plan annuel [61] des mesures qu'ils entendent prendre pour satisfaire aux exigences relatives à la capacité d'interception [62].
- L'amende maximale en cas de violation des exigences est extrêmement élevée – 50 000 $ pour une personne et 10 millions de dollars pour une entreprise [63].
- Le télécommunicateur doit prendre des mesures pour empêcher l'utilisation de ses réseaux et de ses installations de télécommunication pour la perpétration de délits ou pour des activités liées à un délit [64]. Il pourrait donc, dans la plupart des cas, être considéré comme un « agent de l'État ». Le projet de loi C-30 ne prévoit pas la même obligation, mais les télécommunicateurs canadiens pourraient également être considérés comme des agents de l'État depuis l'adoption, en mars 2011, de la *Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet* [65].
- Une disposition prévoit le partage des coûts entre le secteur des télécommunications et les organismes chargés de l'application des lois. Les télécommunicateurs acquittent la majeure partie des frais liés à l'acquisition et au maintien de leur capacité d'interception. De leur côté, les organismes chargés de l'application des lois acquittent les frais de formatage et de production des renseignements. Les détails du partage des coûts sont énoncés dans le contrat conclu entre le télécommunicateur et les organismes chargés de l'application des lois [66].
- La TA1997 précise que l'application d'une norme technique internationale satisfait aux exigences en matière de capacité d'interception [67].
- La TA1997 crée un organisme (Agency Co-ordinator) qui sert de point de contact entre les organismes chargés de l'application des lois et le secteur des télécommunications sur les questions d'interception [68]. Cet organisme est chargé de réunir les commentaires des organismes chargés de l'application des lois concernant la capacité d'interception des fournisseurs. Il offre également des conseils juridiques concernant l'accès légal.

4.2 RENSEIGNEMENTS SUR LES ABONNÉS

À l'instar du projet de loi C-30, la loi australienne permet aux organismes chargés de l'application des lois d'avoir accès à des renseignements sur les abonnés, sans avoir obtenu au préalable un mandat ou une ordonnance judiciaire. Le système en place comporte néanmoins certains éléments particuliers.

Contrairement au projet de loi C-30, le régime australien établit une base de données [69] contenant non seulement le nom, l'adresse et le numéro de téléphone de l'abonné, mais aussi l'emplacement de l'appareil téléphonique et son utilisation (gouvernementale, commerciale, caritative ou personnelle) [70].

Les organismes chargés de l'application des lois peuvent avoir accès à cette base de données pour des motifs liés à la sécurité nationale, à l'application du droit pénal et à la sauvegarde des recettes publiques [71]. Même s'il existe un *ombudsman* chargé d'examiner les plaintes concernant les entreprises de télécommunication et de faire enquête, les mesures de protection proposées dans le projet de loi C-30 semblent avoir une portée plus vaste. Le gouvernement australien veut également mettre en

place un système qui contraindrait les télécommunicateurs à recueillir et à conserver systématiquement les données de transmission. Aucune exigence similaire n'est énoncée dans le projet de loi C-30.

4.3 MANDATS POUR L'INSTALLATION DE DISPOSITIFS DE LOCALISATION

Les articles 14 à 21 de la *Surveillance Devices Act 2004* australienne autorisent les tribunaux à délivrer des ordonnances permettant d'obtenir des numéros de téléphone, des données de localisation et des données de transmission selon des critères semblables à ceux qui sont proposés dans le projet de loi C-30 (soupçon fondé sur des motifs raisonnables). En général, toutefois, ces ordonnances ne peuvent être délivrées que dans le cas d'infractions graves (punissables d'une peine d'emprisonnement maximale de trois ans ou plus)[72]. Le projet de loi C-30 ne prévoit aucune restriction similaire. En outre, la loi australienne exige la présentation de rapports annuels sur l'utilisation de ces ordonnances devant chaque chambre du Parlement. Le projet de loi C-30 ne contient pas une telle exigence.

Le projet de loi 2011 modifiant la loi sur la cybercriminalité permettrait aux organismes australiens d'obtenir et de divulguer des données de transmission dans le cadre d'une enquête menée à l'étranger[73]. Le projet de loi C-30 contient une disposition similaire, qui modifie la *Loi sur l'entraide juridique en matière criminelle*[74].

5 CONCLUSION

La *Convention sur la cybercriminalité* prévoit une collaboration accrue entre les pays et, par conséquent, l'harmonisation des lois en matière d'accès légal. Le projet de loi C-30 s'inspire des lois d'autres pays, principalement des États-Unis, du Royaume-Uni et de l'Australie, tout en établissant un régime propre au Canada. Bien que ses deux éléments fondamentaux – la capacité d'interception et l'ordonnance administrative – se retrouvent également dans les lois américaine, britannique et australienne, certaines particularités le distinguent des autres régimes.

Concernant la capacité d'interception, le projet de loi C-30 est moins ambigu que la loi américaine, qui demeure plutôt vague quant au statut des fournisseurs de services Internet, des universités et des petites entreprises de télécommunications. Cette ambiguïté s'explique, en partie, par le fait que c'est un organisme administratif, la FCC, qui a rédigé les règles de fond.

Il faut noter toutefois qu'une situation semblable aurait pu se produire au Canada si certains éléments du régime avaient été intégrés à des règlements plutôt qu'à une loi. Même s'il est vrai qu'une loi ne peut prévoir toutes les circonstances possibles, il reste que le projet de loi C-30 n'établit pas un cadre suffisamment large pour prévoir le traitement de certaines questions importantes à l'avenir, comme le partage des coûts et les normes techniques d'interception. Le Canada devrait-il suivre l'exemple des États-Unis, en créant un fonds spécial, celui du Royaume-Uni, en conférant un vaste pouvoir discrétionnaire au gouvernement, ou celui de l'Australie, en obligeant les télécommunicateurs à acquitter la quasi-totalité des frais associés à la mise en place et au maintien de leur capacité d'interception?

Concernant les renseignements sur les abonnés, le régime énoncé dans le projet de loi C-30 semble plus restrictif que ceux des trois autres pays. Les types de renseignements qu'un organisme chargé de l'application des lois peut obtenir sans mandat ou sans ordonnance judiciaire sont plus restreints. L'ordonnance administrative prévue au projet de loi ne permettra pas de recueillir bon nombre des renseignements dont la collecte est autorisée dans les autres pays, notamment la date, l'heure et la durée de la communication, les numéros des appareils, les données bancaires, le mode de paiement, les renseignements relatifs aux cartes de crédit (États-Unis et Royaume-Uni) ou les données de localisation du téléphone (Royaume-Uni et Australie). Enfin, le projet de loi C-30 ne crée pas de système de stockage des données de transmission, contrairement aux lois du Royaume-Uni et de l'Australie.

NOTES

1. Voir Erin Shaw et Dominique Valiquet, *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*, publication n° 41-1-C30-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 15 février 2012.

2. Les organismes chargés de l'application des lois (forces policières) et de la sécurité nationale (le SCRS et le Centre de la sécurité des télécommunications) exercent parfois des pouvoirs et des niveaux de supervision judiciaire et administrative distincts. Par souci de concision, l'expression « organismes chargés de l'application des lois » utilisée dans le présent document désigne également des organismes chargés de la sécurité nationale, sauf si le contexte indique clairement le contraire.

3. Appelée couramment « écoute électronique », cette technique est très utile dans les enquêtes sur divers crimes, notamment sur les infractions liées aux stupéfiants. Pour connaître le nombre exact de condamnations obtenues grâce à l'écoute électronique et à d'autres techniques, voir Sécurité publique et Protection civile Canada, *Rapport annuel sur la surveillance électronique – 2004*, n° de cat. : PS1-1/2004F-PDF, Ottawa, Ministre de la Sécurité publique et de la Protection civile, 2005, figures 3 et 4.

4. La Convention est entrée en vigueur le 1er juillet 2004, mais elle n'a pas encore été ratifiée par certains pays, dont l'Afrique du Sud et le Canada. Pour consulter la liste des pays qui l'ont signée et ratifiée, voir le document « Convention sur la cybercriminalité – STCE n° : 185 », Bureau des Traités du Conseil de l'Europe.

5. Un projet de loi approuvé le 12 septembre 2012 devrait probablement permettre à l'Australie de ratifier la Convention. Voir Parlement australien, *Cybercrime Legislation Amendment Bill*.

6. Richard W. Downing, « Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime », *Columbia Journal of Transnational Law*, vol. 43, n° 3, 2005, p. 710, 717 et 718.

7. *Communications Assistance for Law Enforcement Act* (CALEA), Pub. L. n° 103-414, 47 USC 1001-1010, 25 octobre 1994.

8. Voir CALEA; 47 USC 1005, art. 105. Au sujet de l'écoute électronique sans mandat judiciaire autorisée par le président George W. Bush dans le contexte de la sécurité nationale et de la lutte contre le terrorisme, voir James Risen et Eric Lichtblau, « Bush Lets U.S. Spy on Callers Without Courts », *The New York Times*, 16 décembre 2005, p. 1.

9. Les nombreux litiges opposant les organismes chargés de l'application des lois, le secteur des télécommunications et des groupes de défense de la vie privée ont retardé la mise en œuvre des règlements. Ils portent principalement sur les normes techniques, le partage des coûts et la protection de la vie privée. Le débat est loin d'être clos.

10. Le Centre de la sécurité des télécommunications, chargé de recueillir des renseignements étrangers, est protégé contre toute responsabilité criminelle lorsqu'il intercepte des communications privées dans le cadre de ses fonctions principales liées au renseignement.

11. Selon le European Telecommunications Standards Institute (ETSI), « posséder la capacité technique » signifie que le fournisseur de services doit fournir une interface qui permet la transmission de données conservées à un organisme chargé de l'application des lois d'une manière fiable, sécuritaire, rapide et normalisée, tout en perturbant le fournisseur le moins possible et en réduisant ses coûts au minimum. Le Canada a participé à l'élaboration des spécifications techniques de l'ESTI relatives à l'interception légale.

12. Selon la définition donnée au par. 2(1) du projet de loi C-30, les « données de télécommunication » sont les données indiquant l'origine, le type, la direction, la date, l'heure, la durée, le volume, la destination ou la terminaison d'une télécommunication produite ou reçue au moyen d'une installation de télécommunication, et les données indiquant le type de service utilisé. Sont incluses dans cette définition les « données de transmission », qui s'appliquent à la partie 2. La *Convention sur la cybercriminalité* emploie plutôt le terme « données relatives au trafic ». Bien que ces définitions soient assez similaires partout dans le monde, la notion de « données de transmission » peut varier d'un pays à l'autre.

13. CALEA, 47 USC 1002, Titre I, art. 103 et 104.

14. *Ibid*., 47 USC 1001, Titre I, art. 102 et 103.

15. Contrairement au régime proposé dans le projet de loi C-30, il s'agit ici d'un pouvoir discrétionnaire. Le procureur général des États-Unis peut toutefois acquitter les frais dans tous les cas, tandis que le projet de loi C-30 prévoit certaines circonstances dans lesquelles un organisme chargé de l'application des lois ou de la sécurité nationale doit indemniser un télécommunicateur (voir Shaw et Valiquet (2012), par. 2.1.6).

16. CALEA, 47 USC 1008, Titre I, art. 109 et 110. La CALEA établit un montant annuel de 500 millions de dollars pour la période 1995-1998. Selon les télécommunicateurs et l'inspecteur général du ministère de la Justice, le solde de ce montant sera insuffisant. Voir Patricia Moloney Figliola, *Digital Surveillance: The Communications Assistance for Law Enforcement Act*, rapport produit pour le Congrès, RL30677, Congressional Research Service, Library of Congress, Washington, 3 mai 2005, p. 10 et 13.

17. CALEA, 47 USC 1006, Titre I, art. 107. Il s'agit de la disposition « *safe harbor* » en vertu de laquelle la Telecommunications Industry Association, qui représente les fabricants de matériel de télécommunication, a élaboré la norme J-STD-025, appelée aussi la « J-standard », qui a été incorporée aux installations de télécommunication. Le FBI a toutefois jugé que cette norme n'était pas assez inclusive et ne respectait pas les exigences de la CALEA. La FCC a donc obligé les télécommunicateurs à intégrer à leurs réseaux certaines capacités techniques supplémentaires (énumérées dans la « *Punch List* ») avant le 30 juin 2004. Par exemple, les dispositifs doivent pouvoir intercepter des numéros composés après le début de l'appel. Les télécommunicateurs doivent également pouvoir établir un lien entre les données de transmission et le contenu d'une communication interceptée (voir FCC 99-230, *Third Report and Order*, CC Docket No. 97-213, 31 août 1999). Cette dernière exigence est clairement énoncée dans le projet de loi C-30.

18. Declan McCullagh, « FBI Net-wiretapping rules face challenges », *CNet News.com*, 24 octobre 2005.

19. CALEA, 47 USC 1001, Titre I, art. 102, les définitions de « services d'information » et « entreprise de télécommunications »; et art. 103. Voir également Comité des affaires judiciaires, *Telecommunications Carrier Assistance to the Government*, Chambre des représentants, 103e Congrès, 2e session, 4 octobre 1994.

20. En raison également du contexte politique dans lequel a eu lieu le renouvellement de la *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Pub. L. no. 107-56, 111 Stat. 272 (2001).

21. FCC 05-153, *First Report and Order*, CC Docket No. 04-295, 23 septembre 2005.

22. « Voix sur le protocole Internet » (VoIP). Seuls les systèmes connectés au réseau téléphonique public sont touchés (par exemple, les services « Vonage » et « SkypeOut »).

23. Anne Broache, « Feds' Net-wiretap order set to kick in », *CNet News.com*, 11 novembre 2005.

24. L'un des arguments avancés était qu'il n'est pas nécessaire d'élargir la portée de la CALEA pour l'écoute sur Internet – cette pratique avait déjà cours bien avant l'adoption de la loi. Voir Declan McCullagh, « Perspective: Net wiretapping plans under fire », *CNet News.com*, 19 décembre 2005.

25. Voir *R.* c. *Plant*, [1993] 3 R.C.S. 281, p. 293; *R.* c. *Gomboc*, [2010] 3 R.C.S. 211; *R.* c. *McNeice*, 2010 BCSC 1544 (Cour supérieure de la C.-B.); *R.* c. *Brousseau*, 2010 ONSC 6753 (C.S.J. de l'Ontario) (lorsque la divulgation est autorisée en vertu de l'entente avec l'abonné); *R.* c. *Vasic* (2009), 185 C.R.R. (2d) 286 (C.S.J. de l'Ontario) (lorsque la divulgation est autorisée en vertu de l'entente avec l'abonné); *R.* v. *Wilson*, [2009] O.J. n° 1067, 10 février 2009 (C.S.J. 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); *R.* v. *Nguyen* (2004), 20 C.R. (6th) 135 (Cour supérieure de la C.-B.); *R.* v. *Mahmood* (2008), 236 C.C.C. (3d) 3 (C.S.J. de l'Ontario); *R.* v. *Kwok*, [2008] O.J. 2414; (Cour de justice de l'Ontario); et *R.* v. *Cuttell*, 2009 ONCJ 471, 247 C.C.C. (3d) 424 (Cour de justice de l'Ontario).

26. 18 USC 2703(*c*)(1)(E) et (2). Il s'agit d'une « assignation administrative ».

27. Outre le nom, l'adresse, le numéro de téléphone et l'adresse de protocole Internet (IP) de l'abonné (des renseignements également mentionnés dans le projet de loi C-30), le régime américain inclut également la date, l'heure et la durée de la communication, les données téléphoniques, les numéros des appareils, ainsi que le mode de paiement, les données bancaires et le numéro de la carte de crédit.

28. Audience du Comité sénatorial des affaires judiciaires des États-Unis, sous-comité sur le terrorisme, la technologie et la sécurité intérieure, *Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists*, Testimony of Rachel Brand, Principal Deputy Assistant Attorney General, Office of Legal Policy, Département de la Justice des États-Unis, 22 juin 2004.

29. Comprend également la voix sur le protocole Internet (VoIP), comme Skype et FaceTime.

30. 18 USC, ch. 206.

31. 50 USC, ch. 36.

32. Chapitre 23. En vigueur depuis octobre 2000, elle remplace l'*Interception of Communications Act 1985*.

33. Voir la décision *Halford* c. *Royaume-Uni*, 1997, Cour européenne des droits de l'homme (73/1996/692/884).

34. L'exercice de ce pouvoir est soumis à la surveillance du commissaire à l'interception des communications.

35. Gabrielle Garton Grimwood et Christopher Barclay, *The Regulation of Investigatory Powers Bill*, document de recherche 00/25, Bibliothèque de la Chambre des communes, 3 mars 2000, p. 32 et 33.

36. Ministère du Commerce et de l'Industrie, *Building Confidence in Electronic Commerce: A Consultation Document*, URN 99/642, mai 1999.

37. Le ministre de l'Intérieur a le pouvoir d'imposer une telle obligation.

38. RIPA, art. 12 et par. 12(7).

39. *Ibid.*, par. 12(1), 12(10), 12(5) et 12(6). Le Comité consultatif technique (Technical Advisory Board) examinera les normes techniques proposées et leurs répercussions financières sur les activités du fournisseur.

40. *Ibid*., art. 14.

41. *Ibid*., par. 49(2) et 50(2).

42. *Anti-Terrorism Crime and Security Act 2001*, ch. 24, partie 11 : *Retention of Communications Data*. Voir Edgar A. Whitley et Ian Hosein, « Policy discourse and data retention: The technology politics of surveillance in the United Kingdom », *Telecommunications Policy*, vol. 29, 2005. Le 21 février 2006, le Conseil de l'Union européenne a adopté une directive sur la conservation des données de transmission (l'Irlande et la Slovaquie ont voté contre son adoption). Les télécommunicateurs doivent désormais conserver ces données pendant une période allant de six mois à deux ans. Les États membres ont eu 18 mois, à compter de la date d'entrée en vigueur de la directive, pour se conformer aux nouvelles exigences. Voir Parlement européen, *Communications électroniques : données personnelles, protection de la vie privée et accès aux données relatives au trafic à des fins antiterroristes*, 2005-0182(COD).

43. Nom, date de naissance, numéro de téléphone, adresse de facturation, adresse électronique, adresse IP, mode de paiement, numéro de carte de crédit, etc.

44. Numéro de téléphone, identificateur unique, date, heure et durée de l'appel, l'endroit où se trouve le répondant, etc.

45. Adresses IP, adresses électroniques, date, heure, etc.

46. Date, heure, adresses IP, adresses URL. L'adresse URL conservée ne contient que le nom du domaine (p. ex. http://www.parl.gc.ca). Si des caractères suivent le nom du domaine (p. ex. http://www.parl.gc.ca/Search/Results.asp?lawful+access), il s'agit de données relatives au contenu qui ne peuvent donc être conservées systématiquement.

47. Ministère de l'Intérieur du R.-U., *Retention of Communications Data under Part 11: Anti-terrorism, Crime and Security Act 2001 – Voluntary Code of Practice*, Annexe 1.

48. RIPA, par. 22(4) et 25(2).

49. *Ibid*., par. 23(1).

50. *Ibid*., par. 21(4).

51. *Ibid*., par. 22(5) et 22(2). En vertu du projet de loi C-30, des membres désignés des services de police peuvent demander, par écrit, des renseignements liés à toute *fonction policière*, que ce soit l'application des lois fédérales ou provinciales ou de celles d'un État étranger. Les personnes désignées par le SCRS et le commissaire de la concurrence ne peuvent demander que des renseignements liés aux fonctions qu'elles exercent en vertu de la loi habilitante pertinente. Au Royaume-Uni, il est possible de demander des

données de transmission pour d'autres motifs, par exemple dans l'intérêt économique du Royaume-Uni, pour la protection de la santé publique ou pour la perception d'une taxe, d'un droit ou de tout autre impôt.

52. *Ibid*., art. 57 et 65 et les suivants. En plus du Commissaire à la protection de la vie privée, le Canada a également la Commission des plaintes du public contre la GRC (portant sur les activités de la GRC) ainsi que le Comité de surveillance des activités de renseignement de sécurité (concernant les activités du SCRS).

53. *Draft Communications Data Bill*, Parlement du R.-U., Londres, juin 2012.

54. *Ibid*., Préface, p. i.

55. *Ibid*., voir les définitions des termes « *traffic data* », « *use data* » et « *subscriber data* » à l'art. 28 du projet de loi.

56. *Ibid*., art. 9 et 11.

57. RIPA, partie II.

58. *Ibid*., par. 28(2) et 32(2).

59. Comme au Canada, la délivrance d'un mandat pour l'interception en temps réel est assujettie à une réglementation plus sévère.

60. *Telecommunications Act 1997*, parties 13 à 15 et art. 325 à 327. Le ministre des Communications et un organisme spécial (l'Agency Co-ordinator) ont le pouvoir d'exempter un télécommunicateur des obligations relatives à la capacité d'interception. L'ACMA peut également exempter un fournisseur qui met en place un service à l'essai.

61. Appelé le Plan sur la capacité d'interception (*Interception Capability Plan*).

62. *Telecommunications Act 1997*, art. 328 et les suivants. En 2004, certains fournisseurs n'ont pas présenté de plan. Leur cas a été porté à l'attention de l'ACMA, mais aucune accusation n'a été portée. Voir Anthony S. Blunn, *Report of the Review of the Regulation of Access to Communications*, gouvernement de l'Australie, ministère du Procureur général, août 2005, p. 40.

63. *Telecommunications Act 1997*, par. 570(3) et (4). Voir ACMA, *Telecommunications Interception Review – Review of the Longer Term Cost-Effectiveness of Telecommunications Interception Arrangements Under Section 332R of the* Telecommunications Act 1997, juin 1999, p. 33. Le projet de loi C-30 prévoit des amendes maximales de 100 000 $ pour une personne et de 500 000 $ pour une entreprise.

64. *Telecommunications Act 1997*, art. 313.

65. Pour plus de détails sur le projet de loi C-22, voir Dominique Valiquet, *Résumé législatif du projet de loi C-22 : Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet*, publication n^{o} 40-3-C22-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 15 février 2011.

66. *Telecommunications Act 1997*, art. 332K et les suivants. Voir Blunn (2005), p. 49.

67. *Ibid.*, art. 322.

68. *Ibid*., art. 7A.

69. Il s'agit de l'*integrated public number database*. Voir *ibid*., partie 4, annexe 2.

70. *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*, par. 10(4).

71. *Ibid.*, par. 10(8).

72. Voir la définition de « *relevant offences* ».

73. Pour plus de détails sur ce projet de loi, voir Parlement d'Australie, Comité mixte spécial sur la cybercriminalité, *Review of the Cybercrime Legislation Amendment Bill 2011*, Canberra, août 2011.

74. En tant que signataires de la *Convention sur la cybercriminalité*, les États-Unis et le Royaume-Uni ont adopté des dispositions législatives similaires.