BIBLIOTHÈQUE du PARLEMENT
LIBRARY of PARLIAMENT

ÉTUDE GÉNÉRALE

Cybercriminalité : les enjeux

Publication n^{o} 2011-36-F
Le 5 avril 2011

Dominique Valiquet

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

Cybercriminalité : les enjeux
(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 présentent et analysent de façon objective et impartiale diverses questions d'actualité sous différents rapports. Elles 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.

Publication n^{o} 2011-36-F
Ottawa, Canada, Bibliothèque du Parlement (2011)

TABLE DES MATIÈRES

CYBERCRIMINALITÉ : LES ENJEUX

1 LA CYBERCRIMINALITÉ

Dans son *Rapport sur les plans et les priorités 2009-2010*, Sécurité publique et Protection civile Canada comptait l'élaboration d'une stratégie de cybersécurité pangouvernementale au nombre de ses priorités [1]. Cette stratégie a pour objet d'assurer l'intégrité cybernétique du gouvernement, de protéger l'économie et les infrastructures essentielles et de lutter contre la cybercriminalité.

Sa mise en œuvre, qui est en cours, exige la modernisation du cadre législatif canadien et des techniques d'enquête dans un contexte de coopération internationale accrue. Ainsi, les organismes d'application de la loi et ceux chargés de la sécurité nationale [2] pourront avoir accès aux renseignements requis et mener des enquêtes légales aussi bien sur les actes criminels ou terroristes commis au moyen de l'utilisation illégale de nouvelles technologies que sur les organisations criminelles ou terroristes qui utilisent ces technologies pour promouvoir leur cause [3].

1.1 DÉFINITION

Si on parle beaucoup de cybercriminalité, on ne s'entend pas nécessairement sur une définition unique [4]. Toutefois, la définition que propose le Collège canadien de police tend à gagner du terrain : « La cybercriminalité est la criminalité ayant l'ordinateur pour objet ou pour instrument de perpétration principale [5]. »

Entre autres choses, elle permet de classer les cybercrimes en deux catégories pratiques :

- Le *délit informatique pur*, où l'ordinateur est l'objet du crime. Cette catégorie comprend de nouvelles infractions précises visant les systèmes et les réseaux informatiques, par exemple le piratage informatique, les attaques pour déni de service [6] et la propagation malveillante de virus informatiques.
- Le *délit assisté par ordinateur*, où l'ordinateur est l'instrument de perpétration du crime. Cette catégorie concerne l'utilisation de l'ordinateur pour perpétrer des infractions traditionnelles, qu'il s'agisse de pornographie juvénile, de harcèlement, de fraude ou de trafic de drogues.

1.2 DÉFIS

La cybercriminalité est une source de nouveaux défis pour le législateur et pour les organismes d'application de la loi, notamment :

- l'application des lois canadiennes dans le cyberespace et la coopération internationale dans les enquêtes sur la cybercriminalité;
- la modernisation – mise à jour et création – des infractions pour inclure les nouveaux délits informatiques ou les nouvelles formes d'infractions;

- la modernisation des techniques d'enquête.

La présente publication donne un bref aperçu de divers éléments de ces trois défis.

2 ASPECTS INTERNATIONAUX

Selon le principe général de territorialité applicable au Canada, personne ne doit être déclaré coupable au pays d'une infraction entièrement commise à l'étranger [7]. Il y a exception dans le cas de certaines infractions précises comme la torture, le terrorisme ou le tourisme sexuel impliquant des enfants [8].

La cybercriminalité ne connaît toutefois aucune frontière, ce qui complique grandement les enquêtes policières. La coopération entre pays est donc essentielle pour lutter efficacement contre cette forme de criminalité.

2.1 CHAMP D'APPLICATION DES LOIS CANADIENNES

Les pays signataires de la *Convention sur la cybercriminalité* (la Convention) [9], dont fait partie le Canada [10], doivent poursuivre les cybercrimes commis sur leur territoire [11]. Ainsi, un pays pourrait revendiquer une compétence territoriale dans le cas où le système informatique attaqué se trouverait sur son territoire, même si l'auteur de l'attaque ne s'y trouvait pas.

L'Australie, par exemple, a expressément conféré à ses autorités le pouvoir de poursuivre un pirate informatique qui attaque, de l'étranger, un ordinateur situé en Australie [12]. Les États-Unis ont aussi modifié leur législation afin de permettre les poursuites contre les personnes à l'étranger qui attaquent des ordinateurs aux États-Unis et les personnes aux États-Unis qui attaquent des ordinateurs situés dans d'autres pays [13]. Cette modification permet également aux autorités américaines d'enquêter sur le piratage informatique provenant de l'étranger, si un ordinateur se trouvant aux États-Unis est utilisé comme intermédiaire [14].

Afin d'éliminer les « zones sûres », la Convention exige que les pays signataires qui n'extradent pas un délinquant à cause de sa nationalité aient la compétence pour le poursuivre sur leur propre territoire [15]. Bien que le Canada poursuive les infractions perpétrées sur son territoire et extrade ses nationaux, l'application des lois canadiennes aux infractions commises dans le cyberespace gagnerait à être clarifiée.

2.2 TRAITÉS D'ENTRAIDE JURIDIQUE

En vertu des traités d'entraide juridique bilatéraux et des conventions multilatérales, le Canada peut recevoir et fournir de l'aide pour rassembler des preuves dans les affaires criminelles impliquant d'autres pays. Dans l'un et l'autre cas, il aura recours, au besoin, à des mesures coercitives. Toutefois, ces mécanismes entraînent souvent de trop longs délais, selon ce que signalent les organismes d'application de la loi et poursuivants canadiens [16]. Considérant la rapidité avec laquelle les données informatiques peuvent être déplacées, modifiées ou supprimées, une solution

pourrait être de mettre en place une procédure expéditive de conservation des éléments de preuve entre les mains des partenaires étrangers du Canada.

Par ailleurs, dans le cadre de poursuites en matière de cybercriminalité, la preuve provient souvent de nombreux États différents. Les témoins qui se trouvent dans d'autres pays doivent donc venir au Canada afin de témoigner devant un tribunal. Dans un rapport préparé pour l'Association canadienne des commissions de police, on mentionne qu'une modification à la *Loi sur la preuve au Canada* permettant la preuve par affidavit ou par vidéo serait à considérer dans ces cas[17].

3 MODERNISATION DES INFRACTIONS

Bien que la plupart des cybercrimes existent déjà en droit canadien, l'émergence de la cybercriminalité donne à penser qu'une révision des infractions criminelles qu'il prévoit et leur mise à jour, au besoin, pourraient être nécessaires.

3.1 VIRUS

Actuellement, seules la propagation d'un virus informatique ou d'autres dispositifs malveillants (p. ex. les vers et les chevaux de Troie) et la tentative de propagation constituent des infractions[18].

Afin de ratifier la Convention, le Canada devrait modifier son *Code criminel* (le *Code*) pour que la création, l'importation, la vente, la mise à disposition ou la possession d'un virus ou d'un autre dispositif malveillant dans le but de commettre un cybercrime constituent des infractions en droit canadien.

3.2 PORNOGRAPHIE JUVÉNILE

Les dispositions actuelles du *Code* relatives à la pornographie juvénile semblent bien adaptées à la réalité du cyberespace. En effet, en plus de la production et de la possession de la pornographie juvénile, le fait d'y accéder – par exemple en visitant une page Web – ou de la rendre accessible – par exemple en utilisant un programme de partage de fichiers (p. ex. P2P) – constituent des infractions.

Afin d'aider les services de police à combattre cet important cybercrime, un groupe de travail fédéral, provincial et territorial sur la cybercriminalité a étudié la possibilité d'imposer aux fournisseurs de service Internet (FSI) l'obligation de signaler les incidents impliquant l'exploitation des enfants qui se produisent sur leur réseau.

En juin 2008, l'Assemblée législative du Manitoba a sanctionné une loi[19] obligeant quiconque à signaler à Cyberaide.ca[20] tout cas de pornographie juvénile. L'Alberta, la Nouvelle-Écosse et l'Ontario lui ont rapidement emboîté le pas en adoptant des lois semblables[21].

Sur la scène fédérale, le projet de loi C-22[22], qui a reçu la sanction royale le 23 mars 2011, impose aux FSI et aux autres personnes qui fournissent des services Internet

(p. ex. Facebook, Google et Hotmail) l'obligation de rapporter tout incident concernant la pornographie juvénile [23].

Les États-Unis [24] et l'Australie [25] se sont dotés, en 2002 et 2005 respectivement, de lois imposant ce type d'obligation aux personnes qui fournissent des services de télécommunication (les « télécommunicateurs »).

3.3 VOL D'IDENTITÉ

Le *Code* vise la plupart des utilisations frauduleuses de renseignements personnels par les voleurs d'identité. En revanche, avant l'entrée en vigueur du projet de loi S-4 [26] en janvier 2010, il ne s'appliquait pas à la collecte, à la possession ou au trafic illicite de renseignements personnels pour un futur usage criminel (sauf en ce qui concerne les cartes de crédit et les mots de passe des ordinateurs).

Le projet de loi S-4 comble cette lacune. Il crée deux nouvelles infractions : le vol d'identité et le trafic de renseignements identificateurs. En plus d'avoir mis à jour les infractions relatives aux cartes de crédit, le projet de loi a prévu la possibilité pour le juge d'ordonner au délinquant de dédommager la victime d'un vol d'identité [27].

3.4 POURRIELS

Le pourriel est un message électronique non sollicité. De nuisance qu'il était, le pourriel est devenu un véhicule pour commettre des infractions telles que la propagation des virus, la fraude ou le vol d'identité. Bien que le pourriel représente environ 80 % du courriel mondial [28], le Canada demeurait, jusqu'à tout récemment, le seul pays du G8 sans loi antipourriel.

En mai 2005, le Groupe de travail canadien sur le pourriel a recommandé l'adoption d'une loi pour interdire les messages électroniques commerciaux non sollicités [29]. Le projet de loi C-28 [30], qui a reçu la sanction royale le 15 décembre 2010, a mis en place un régime de réglementation clair, assorti de sanctions administratives pécuniaires, concernant aussi bien le pourriel que les menaces connexes provenant de contacts électroniques non sollicités, dont le vol d'identité, l'hameçonnage [31], les logiciels espions [32], les virus et les réseaux d'ordinateurs zombies [33]. Il accorde également un droit supplémentaire de poursuite au civil aux entreprises et aux consommateurs visés par les auteurs de ces activités [34].

3.5 AUTRES INFRACTIONS ÉMERGENTES DANS LE CYBERESPACE

Dans le cadre d'un sondage effectué en 2008 pour le compte de l'Association canadienne des commissions de police auprès d'organismes d'application de la loi, de procureurs de la Couronne et d'autres représentants des gouvernements au Canada, les répondants ont soulevé deux enjeux de plus en plus importants : la cyberintimidation des enfants et le crime organisé sur Internet [35].

Bien que les infractions actuelles semblent s'appliquer à ces phénomènes, il pourrait être important de les étudier plus en profondeur.

4 MODERNISATION DES TECHNIQUES D'ENQUÊTE

Selon les organismes d'application de la loi, les nouvelles technologies représentent souvent des obstacles à l'interception légale des communications – que l'on pense notamment à l'anonymat des usagers, aux messages cryptés ou au caractère relativement éphémère des informations. Les sections suivantes présentent très brièvement ces questions ainsi que des pistes de solutions qui pourraient être envisagées [36].

4.1 CAPACITÉ D'INTERCEPTION

Il n'existe, à l'heure actuelle, aucune loi canadienne contraignant tous les télécommunicateurs à utiliser des appareils dotés de la capacité d'intercepter les communications [37]. Une mesure législative pourrait remédier à cette absence de norme concernant la capacité d'interception des télécommunicateurs. Elle pourrait obliger tous ceux qui fournissent des services de télécommunications, par exemple les FSI et les fabricants d'appareils comme le BlackBerry, à utiliser une technologie permettant aux organismes d'application de la loi d'intercepter les télécommunications à des fins d'enquête, après en avoir obtenu l'autorisation judiciaire [38].

L'Australie, les États-Unis et le Royame-Uni, entre autres, ont adopté des mesures semblables depuis plus de 10 ans déjà [39].

4.2 DEMANDE DE RENSEIGNEMENTS SUR LES ABONNÉS

Actuellement, les organismes d'application de la loi doivent généralement être munis d'un mandat afin de contraindre les télécommunicateurs à leur transmettre des renseignements personnels sur leurs clients [40]. Ainsi, un service de police qui détient une adresse de protocole Internet (adresse IP) [41] associée à la perpétration d'une infraction doit obtenir un mandat afin de contraindre le télécommunicateur à lui fournir le nom de l'abonné lié à l'adresse IP. La demande de mandat doit toutefois comprendre le nom du suspect de l'infraction.

Pour remédier à ce problème, on pourrait mettre en place un régime spécial permettant aux organismes d'application de la loi de contraindre – sans mandat, mais à certaines conditions – un télécommunicateur à leur fournir des informations de base identifiant un de leurs abonnés (p. ex. nom, adresse IP, adresse de courrier électronique ou numéro de téléphone) [42]. Certains soutiennent que cette demande de renseignements devrait toujours recevoir l'approbation préalable d'un juge [43].

Il est intéressant de noter que la Cour supérieure de justice de l'Ontario, dans une décision rendue en février 2009 [44], a jugé que les abonnés ne possèdent pas une expectative raisonnable de vie privée à l'égard des informations de base détenues par leur FSI. Un peu plus tard la même année, la Cour de justice de l'Ontario a précisé la question. Dans l'affaire *R.* v. *Cuttell* [45], elle a décidé qu'un FSI peut divulguer aux forces policières les noms et adresses de ses abonnés sans mandat, mais uniquement si le contrat de services de télécommunication le liant à ses abonnés le permet. Or la plupart des contrats des grandes entreprises de télécommunication au Canada le permettent.

Récemment, la Cour suprême de la Colombie-Britannique – d'avis qu'un FSI qui reçoit une demande d'un corps de police visant l'accès à des renseignements sur ses abonnés ne constitue pas un « agent de l'État » – a jugé qu'un FSI peut volontairement fournir aux policiers ces renseignements sur simple demande, c'est-à-dire sans autorisation judiciaire préalable [46].

Étant donné l'état incertain de la jurisprudence sur la nécessité d'un mandat, la question demeurera probablement ouverte jusqu'au moment où la Cour suprême du Canada sera appelée à trancher.

4.3 OBLIGATION DE CONSERVATION DES DONNÉES DE TÉLÉCOMMUNICATION

Le 15 mars 2006, l'Union européenne a adopté la Directive 2006/24/CE sur la conservation de données de télécommunication [47]. Cette directive oblige les télécommunicateurs à conserver le type de données visé pour une période de six mois à deux ans et à donner aux autorités nationales accès à ces données à des fins de détection et de poursuite d'infractions graves.

Au Canada, les télécommunicateurs ne sont pas contraints de recueillir ni de conserver des renseignements sur l'usage de leurs services que font leurs abonnés, entre autres quand ils naviguent sur Internet.

4.4 ANONYMAT DES SERVICES

Les organismes d'application de la loi considèrent que les services cellulaires prépayés, les cartes d'accès Internet, les cafés Internet et les terminaux d'accès à Internet dans les bibliothèques publiques compliquent la tâche des enquêteurs, car ils permettent aux usagers de demeurer anonymes.

À l'heure actuelle, les télécommunicateurs ne sont nullement obligés de vérifier l'identité de leurs usagers.

4.5 ORDONNANCE DE PRÉSERVATION

Les renseignements que l'on trouve sur Internet peuvent facilement et rapidement être détruits ou modifiés, ce qui peut occasionner une perte d'éléments de preuve. Une façon de remédier à ce problème serait d'ajouter une ordonnance de préservation au *Code* [48]. Il s'agirait d'une ordonnance judiciaire temporaire – en vigueur pour la durée nécessaire à l'obtention d'un mandat de perquisition – qui enjoindrait à un télécommunicateur de conserver des renseignements à propos d'une télécommunication particulière ou d'une personne visée.

L'ancien projet de loi C-51 [49], mort au *Feuilleton* lors du déclenchement des élections générales le 26 mars 2011, prévoyait de telles ordonnances relativement à la conservation de données informatiques [50].

4.6 ORDONNANCE DE COMMUNICATION

L'ordonnance de communication ressemble au mandat de perquisition, car tout comme celui-ci, elle est délivrée par un juge. Une caractéristique les distingue toutefois : dans le cas de l'ordonnance de communication, c'est la personne qui possède l'information qui, sur demande, la produit, alors que dans celui du mandat de perquisition, c'est l'organisme d'application de la loi qui se rend sur place pour obtenir les renseignements recherchés au moyen d'une saisie. Munis d'une ordonnance de communication, les organismes d'application de la loi peuvent ainsi obtenir plus facilement des documents se trouvant dans un autre pays.

Le *Code* prévoit actuellement une procédure pour obtenir une ordonnance de communication générale, c'est-à-dire une ordonnance qui s'applique, peu importe le type de renseignement qu'un organisme d'application de la loi recherche [51]. La délivrance d'une telle ordonnance est basée sur l'existence de motifs raisonnables de *croire* qu'une infraction a été commise. Puisque certains croient que l'expectative de vie privée est moins grande à l'égard des données de télécommunication qu'à l'égard des autres types de renseignements, on pourrait envisager de créer une ordonnance de communication spécifiquement pour obtenir des données de télécommunication [52] selon un critère moins exigeant, soit l'existence de motifs raisonnables de *soupçonner* qu'une infraction a été commise [53].

L'ancien projet de loi C-51, dont nous avons parlé plus haut, prévoyait une telle ordonnance relativement à la communication de certains types d'information, par exemple les données de transmission et de localisation.

4.7 INTERCEPTION DU COURRIER ÉLECTRONIQUE

Le traitement du courrier électronique fait l'objet d'un débat : l'organisme d'application de la loi qui désire obtenir le courrier électronique d'un suspect doit-il demander un mandat de perquisition ou une autorisation d'interception en vertu de la partie VI du *Code*? (Le régime de la partie VI – qui permet aux organisations policières d'intercepter une « communication privée » [54] – est plus exigeant que celui relatif aux mandats de perquisition.)

Si un simple courriel constitue bel et bien une communication, il n'est pas certain que son auteur puisse raisonnablement s'attendre à ce que seul son destinataire en prenne connaissance – donc qu'il soit « privé ». En effet, puisque, d'une part, le courriel peut facilement être intercepté [55] et que, d'autre part, son auteur peut facilement recourir aux technologies de cryptage pour en assurer la confidentialité, le courriel ne pourrait être qualifié de « communication privée » au sens du *Code* [56].

En revanche, il n'est pas facile de voir pourquoi ce raisonnement ne s'appliquerait pas aussi aux communications téléphoniques : pourquoi existerait-il une différence entre la protection accordée à un courriel et celle accordée à une communication téléphonique? La question se pose d'autant plus qu'un message électronique peut lui aussi renfermer diverses informations et contenir des renseignements personnels délicats.

4.8 CRYPTAGE

Le cryptage est une opération qui permet de rendre une communication inintelligible pour ceux qui ne possèdent pas la clé qui permet de la décoder. Pour répondre à la nécessité d'assurer la confidentialité des messages transmis sur Internet, les technologies de cryptage sont devenues de plus en plus sophistiquées et, du coup, de plus en plus accessibles.

Si ces technologies sont utiles pour protéger les communications légitimes sur Internet, elles représentent aussi un obstacle à l'interception légale des communications par les organismes d'application de la loi dans le cadre d'enquêtes criminelles.

Par conséquent, on pourrait exiger des télécommunicateurs qu'ils donnent accès aux communications en clair (décodées) aux organismes d'application de la loi, et ce, peu importe la technologie utilisée par les télécommunicateurs[57]. On pourrait aussi exiger que toutes les technologies de cryptage contiennent une clé de décryptage à laquelle les organismes d'application de loi auraient accès. Cette mesure soulève toutefois des questions relatives à la protection de la vie privée.

NOTES

1. Sécurité publique et Protection civile Canada, *Rapport sur les plans et les priorités 2009-2010*, Ottawa, 2009, p. 10.
2. Dans le présent document, nous utiliserons le terme « organismes d'application de la loi » pour comprendre à la fois, selon le contexte, les organismes d'application de la loi et ceux chargés de la sécurité nationale.
3. Sécurité publique et Protection civile Canada (2009), p. 19.
4. Cette absence de définition constitue un obstacle à la collecte de statistiques.
5. Collège canadien de police, cité dans Centre canadien de la statistique juridique, *Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police*, n° 85-558-XIF au catalogue de Statistique Canada, décembre 2002, p. 6.
6. Il s'agit d'attaques sur un système ou un réseau informatique qui entraînent une perte de service pour les usagers.
7. *Code criminel* (le *Code*), L.R.C. 1985, ch. C-46, par. 6(2). Voir aussi *Libman c. La Reine*, [1985] 2 R.C.S. 178, où la Cour suprême du Canada traite du « lien réel et important » entre une infraction et un pays.
8. Les exceptions à la règle générale de territorialité se trouvent à l'art. 7 du *Code*.
9. Conseil de l'Europe, *Convention sur la cybercriminalité* (la Convention), 23 novembre 2001.
10. Le Canada a signé la Convention le 23 novembre 2001.
11. Convention, art. 22.
12. 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. 737.

13. *Ibid.* En conséquence, un réseau fonctionnant tous les jours 24 heures sur 24 a été créé afin de mettre en place une procédure expéditive et efficace de collaboration entre les organismes d'application de la loi des pays du G-8 (voir l'entente de Moscou du G-8 : Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscou, 19 et 20 octobre 1999, *Communiqué*); la Convention prévoit aussi un tel réseau.

14. Afin de dissimuler leurs traces, les pirates informatiques utilisent souvent un réseau d'ordinateurs intermédiaires (on parle alors d'ordinateurs « zombies ») entre leur propre ordinateur et l'ordinateur attaqué.

15. Convention, art. 22.

16. Deloitte & Touche LLP, *A report on cybercrime in Canada*, rapport préparé pour l'Association canadienne des commissions de police, Toronto, 29 avril 2008, p. 14. Certaines organisations d'application de la loi préféreraient donc faire directement appel à la coopération d'entreprises privées situées dans l'autre pays. Pensons à Microsoft qui gère les serveurs pour Hotmail aux États-Unis.

17. *Ibid.*, p. 14.

18. *Code*, al. 342.1(1)*c*) et par. 430(1.1).

19. Manitoba, *Loi modifiant la Loi sur les services à l'enfant et à la famille (obligation de signaler la pornographie juvénile)*, par. 18(1.0.1).

20. Cyberaide.ca est le service pancanadien de signalement d'enfants exploités sexuellement sur Internet.

21. Alberta, *Mandatory Reporting of Child Pornography Act*, S.A. 2010, ch. M-3.3; Nouvelle-Écosse, *Child Pornography Reporting Act*, 2008, ch. 35, art. 1; Ontario, *Loi sur les services à l'enfance et à la famille*, L.R.O. 1990, ch. C.11, par. 72(1.1).

22. Projet de loi C-22 : Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet, 3e session, 40e législature.

23. Pour plus d'informations à ce sujet, 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 no 40-3-C22-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, révisé le 15 février 2011.

24. États-Unis, *United States Code* (USC), Title 18, Chapter 110, art. 2258A.

25. Australie, *Criminal Code Act 1995, Schedule*, art. 474.25.

26. Projet de loi S-4 : Loi modifiant le Code criminel (vol d'identité et inconduites connexes), 2e session, 40e législature.

27. Pour de plus amples renseignements sur le projet de loi S-4, voir Nancy Holmes et Dominique Valiquet, *Résumé législatif du projet de loi S-4 : Loi modifiant le Code criminel (vol d'identité et inconduites connexes)*, publication no LS-637F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, révisé le 5 juin 2009.

28. *Ibid*.

29. Canada, Groupe de travail sur le pourriel, *Freinons le pourriel : Créer un Internet plus fort et plus sécuritaire – Rapport du Groupe de travail sur le pourriel*, Industrie Canada, mai 2005.

30. Projet de loi C-28 : Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent

l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications, 3e session, 40e législature.

31. L'hameçonnage est une tentative d'escroquerie par courriel basée sur l'usurpation d'identité d'une personne ou d'une organisation de confiance, dans le but de voler des renseignements personnels.

32. Le logiciel espion est un programme qui, à l'insu de l'utilisateur et sans sa permission, emploie son ordinateur pour recueillir des données personnelles et en modifier le fonctionnement.

33. Un « zombie » est un ordinateur dans lequel fonctionne un virus permettant au créateur, au distributeur ou au contrôleur du virus de l'activer à distance; un réseau d'ordinateurs « zombies » sert à envoyer du pourriel ou à d'autres fins.

34. Pour plus d'informations sur le projet de loi C-28, voir Alysia Davies et Terrence J. Thomas, *Résumé législatif du projet de loi C-28 : Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique*, publication no 40-3-C28-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, révisé le 4 février 2011.

35. Association canadienne des commissions de police (2008), p. 11. Notons que l'entraide internationale en matière de crime organisé passera dans bien des cas par la *Convention des Nations Unies contre la criminalité transnationale organisée et protocoles s'y rapportant* (Convention de Palerme). Voir François Blanchette, « Entraide juridique et cybercriminalité au Canada : le cadre légal national et international », dans *Legal.TI, droit et technologies de l'information : Devenir aujourd'hui l'avocat de demain*, Cowansville, Éditions Yvon Blais, 2008, p. 18 et 19.

36. La plupart des mesures présentées proviennent de consultations publiques menées par le gouvernement fédéral lors de l'élaboration de l'ancien projet de loi C-74 (Loi sur la modernisation des techniques d'enquête, 1re session, 38e législature) entre 2002 et 2005. Le projet de loi C-74 a été présenté en novembre 2005 et est mort au *Feuilleton* avant la deuxième lecture à la Chambre des communes.

37. Seuls les titulaires de licence qui utilisent les fréquences radio pour des systèmes de téléphonie vocale sans fil doivent, depuis 1996, détenir des installations permettant de telles interceptions. Il n'existe aucune obligation semblable pour les autres télécommunicateurs.

38. Les anciens projets de loi C-74 (voir note 36) et C-52 (Loi régissant les installations de télécommunication aux fins de soutien aux enquêtes, 3e session, 40e législature, mort au *Feuilleton* le 26 mars 2011) prévoyaient une obligation semblable à l'égard des personnes qui fournissent des services de télécommunication, mais non à l'égard des fabricants d'appareils.

39. Pour plus d'informations à ce sujet, voir Dominique Valiquet, *Télécommunications et accès légal : II. La situation législative aux États-Unis, au Royaume-Uni et en Australie*, publication no 2005-66-F, Ottawa, Service d'information et de recherche parlementaires,Bibliothèque du Parlement, 28 février 2006.

40. Voir l'al. 7(3)*c.1*) de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

41. L'adresse IP peut être fixe ou différer à chaque branchement (« dynamique »).

42. Les anciens projets de loi C-74 (voir note 36) et C-52 (voir note 38) prévoyaient une telle mesure.

43. En 2007, le gouvernement appuyait cette position. Voir Carly Weeks, « Warrant Needed to Pull Data on Internet Users: Day », *Ottawa Citizen*, 14 septembre 2007.

44. *R.* v. *Wilson* (10 février 2009), n° 4191/08. Selon la Cour, le nom et l'adresse d'un abonné ne révèlent pas de détails intimes sur le mode de vie ou les choix personnels de l'abonné (voir *R.* c. *Plant*, [1993] 3 R.C.S. 281, et *R.* c. *Gomboc*, [2010] 3 R.C.S. 211). Auparavant, la Cour de justice de l'Ontario avait rendu une décision contraire dans *R.* v. *Kwok*, [2008] O.J. 2414.

45. *R.* v. *Cuttell*, 2009 ONCJ 471, [Cour de justice de l'Ontario] (2009 CarswellOnt 5896).

46. *R.* v. *McNeice*, 2010 BCSC 1544 [Cour suprême de la Colombie-Britannique].

47. « Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 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 », *Journal officiel de l'Union européenne,* L105/54, 13 avril 2006. Les données de télécommunication sont, essentiellement, des données qui indiquent l'origine, la destination, la date, l'heure, la durée et la localisation d'une télécommunication. Elles ne révèlent pas le contenu d'une télécommunication. On parle également de « données relatives au trafic », de « données de transmission » ou de « données de communication ».

48. Ce type de mesure est prévu par la *Convention sur la cybercriminalité*.

49. Projet de loi C-51 : Loi concernant le Code criminel, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle, 3e session, 40e législature.

50. Pour plus d'informations sur le projet de loi C-51 (40e législature, 3e session), voir Dominique Valiquet et Katherine Simonds, *Résumé législatif du projet de loi C-51 : Loi sur les pouvoirs d'enquête au 21e siècle*, Service d'information et de recherche parlementaires, publication n° 40-3-C51-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 3 février 2011.

51. *Code*, art. 487.012. Une telle ordonnance est également prévue par la *Loi sur la concurrence*, al. 11(1)*b*).

52. Ce type de mesure est prévu par la *Convention sur la cybercriminalité*.

53. Le *Code* utilise déjà le critère des *motifs raisonnables de soupçonner* dans le cas d'ordonnances de production des registres d'appels téléphoniques (par. 492.2(2)) et d'informations bancaires (par. 487.013(1) et (4)), de même que dans le dans le cas du mandat pour installer un dispositif de localisation (par. 492.1(1)).

54. L'art. 183 du *Code* définit ainsi une « communication privée » :

> Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.

55. Voir *R.* v. *Weir*, [1998] 8 W.W.R. 228 (ABQB) [Cour du Banc de la Reine de l'Alberta].

56. Robert W. Hubbard, Peter M. Brauti et Scott K. Fenton, *Wiretapping and Other Electronic Surveillance: Law and Procedure*, Aurora (Ontario), Canada Law Book, vol. 2, mars 2008, p. 15-20.

57. Les anciens projets de loi C-74 (voir note 36) et C-52 (voir note 38) prévoyaient une mesure semblable.