BIBLIOTHÈQUE du PARLEMENT
LIBRARY of PARLIAMENT

RÉSUMÉ LÉGISLATIF

Projet de loi C-51 :
Loi sur les pouvoirs d'enquête au 21e siècle

Publication no 40-3-C51-F
Le 3 février 2011

Dominique Valiquet

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

Katherine Simonds

Division des affaires internationales, du commerce et des finances
Service d'information et de recherche parlementaires

Résumé législatif du projet de loi C-51

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

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

This publication is also available in English.

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

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

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

Publication n^{o} 40-3-C51-F
Ottawa, Canada, Bibliothèque du Parlement (2011)

TABLE DES MATIÈRES

RÉSUMÉ LÉGISLATIF DU PROJET DE LOI C-51 : LOI SUR LES POUVOIRS D'ENQUÊTE AU 21E SIÈCLE

1 CONTEXTE

1.1 OBJETS DU PROJET DE LOI

Le projet de loi C-51 : Loi modifiant le Code criminel, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle (titre abrégé : « Loi sur les pouvoirs d'enquête au 21e siècle ») a été déposé le 1er novembre 2010 à la Chambre des communes par le ministre de la Justice, l'honorable Robert Douglas Nicholson, ainsi que Dave MacKenzie, secrétaire parlementaire du ministre de la Sécurité publique, et Daniel Petit, secrétaire parlementaire du ministre de la Justice.

Le projet de loi vise à moderniser certaines infractions du *Code criminel* (le *Code*) et de la *Loi sur la concurrence* en tenant compte des nouvelles technologies de communication et à munir les organismes d'application de la loi de nouveaux outils d'enquête adaptés aux délits informatiques. Afin de faciliter la collaboration avec les organismes étrangers d'application de la loi, le projet de loi modifie également la *Loi sur l'entraide juridique en matière criminelle*. Selon le ministère de la Justice, les nouveaux pouvoirs d'enquête proposés dans le projet de loi donnent aux organismes d'application de la loi la capacité de s'attaquer aux organisations criminelles et aux activités terroristes en ligne de la façon suivante :

- En permettant aux policiers d'obtenir tous les renseignements relatifs aux nœuds de réseau et aux pays qui ont participé à la transmission de données constituant une communication de façon à déterminer l'origine de celle-ci et à remonter jusqu'à un suspect. Des demandes d'autorisation judiciaire seront requises pour obtenir les données de transmission, lesquelles portent sur l'acheminement des communications, mais n'incluent pas la teneur d'une communication privée.
- En exigeant d'un fournisseur de services de télécommunication qu'il conserve temporairement des données de manière à ce que celles-ci ne soient pas perdues ou supprimées pendant le temps qu'il faut aux organismes d'application de la loi pour revenir avec un mandat de perquisition ou une ordonnance de production afin de les obtenir.
- En rendant illégale la possession d'un virus informatique en vue de commettre une infraction de méfait.
- En améliorant la collaboration internationale pour faciliter les enquêtes et les poursuites à l'égard des crimes qui traversent les frontières du Canada[1].

Le projet de loi C-51 est identique au projet de loi C-46, déposé à la Chambre des communes le 18 juin 2009 au cours de la 2e session de la 40e législature, sauf qu'il ne reprend pas les dispositions relatives aux infractions commises contre des enfants. De telles dispositions sont proposées dans l'actuel projet de loi C-54 : Loi modifiant le Code criminel (infractions d'ordre sexuel à l'égard d'enfants)[2].
Les mesures législatives proposées complètent celles des projets de loi C-52 :

Loi régissant les installations de télécommunication aux fins de soutien aux enquêtes et C-50 : Loi modifiant le Code criminel (interception de communications privées et mandats et ordonnances connexes), qui abordent divers aspects du régime d'accès légal proposé [3].

1.2 PRINCIPALES MODIFICATIONS APPORTÉES PAR LE PROJET DE LOI

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

- à préciser 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);
- à créer l'infraction de possession d'un virus informatique dans le but de commettre un méfait (art. 10);
- 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. 13);
- 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. 13);
- à créer des mandats qui permettront d'obtenir des données de transmission en temps réel et d'activer à distance des dispositifs de localisation se trouvant dans certains types de technologie (art. 17);
- à moderniser les infractions de pratiques commerciales trompeuses prévues dans la *Loi sur la concurrence* (art. 24 à 26);
- 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. 32).

Plusieurs dispositions du projet de loi s'inspirent des consultations publiques sur l'accès légal tenues par des représentants de Justice Canada, d'Industrie Canada et du Solliciteur général du Canada en 2002 [4], notamment celles relatives aux ordonnances de préservation et de communication.

1.3 *CONVENTION SUR LA CYBERCRIMINALITÉ*

Le Canada a signé la *Convention sur la cybercriminalité* du Conseil de l'Europe en novembre 2001, ainsi que son protocole additionnel sur la propagande haineuse en juillet 2005. La Convention criminalise certaines infractions commises à l'aide de systèmes informatiques et prévoit des outils juridiques adaptés aux nouvelles technologies, comme des ordonnances de préservation et de communication [5].

La Convention prévoit également une ordonnance de produire des données relatives aux abonnés [6], qui présente certaines similitudes avec la demande de renseignements sur les abonnés prévue par le projet de loi C-52 [7], déposé en même temps

que le projet de loi C-51. La combinaison des projets de loi C-51 et C-52 permettra donc au Canada de ratifier la *Convention sur la cybercriminalité* et son protocole additionnel.

2 DESCRIPTION ET ANALYSE

2.1 MODIFICATIONS AU *CODE CRIMINEL*

2.1.1 MODERNISATION DES INFRACTIONS

2.1.1.1 PROPAGANDE HAINEUSE (ART. 4 ET 5)

Les infractions de propagande haineuse doivent être commises à l'égard d'un « groupe identifiable ». L'article 4 du projet de loi ajoute l'origine nationale à la définition actuelle de « groupe identifiable[8] ».

L'article 5 du projet de loi précise que les infractions d'incitation publique à la haine et de fomenter volontairement la haine peuvent être commises par tout moyen de communication et comprennent le fait de rendre accessible du matériel haineux, par exemple en créant un lien hypertexte qui dirigerait les internautes vers un site Web affichant du matériel haineux.

2.1.1.2 DISPOSITIF POUR VOLER DES SERVICES DE TÉLÉCOMMUNICATION (ART. 8)

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 8 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.

2.1.1.3 VIRUS INFORMATIQUE (ART. 10)

Selon les dispositions actuelles du *Code*, seules la propagation d'un virus informatique[9] ou la tentative de propagation constituent une infraction[10]. Conformément aux exigences de la *Convention sur la cybercriminalité*[11], l'article 10 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.

2.1.1.4 COMMUNICATIONS FAUSSES, INDÉCENTES OU HARCELANTES (ART. 11)

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 référence à certaines technologies de communication, utilisées pour commettre ces infractions, comme le télégramme, la radio et le téléphone[12]. L'article 11 du projet de loi modifie ces infractions en supprimant les références à ces technologies de communication

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

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.

2.1.2 Nouveaux outils d'enquête

2.1.2.1 Ordre et ordonnance de préservation (art. 13)

Les renseignements sous forme électronique peuvent être détruits ou modifiés facilement et rapidement. L'article 13 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 fournisseur de services de télécommunication (FST), de sauvegarder des « données informatiques [13] » qui sont en « sa possession ou à sa disposition [14] » au moment où l'ordre ou l'ordonnance est reçu. Toutefois, un FST 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 [15], qui contraint les FST 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 FST uniquement s'il existe des *motifs raisonnables de soupçonner* [16] qu'une infraction a été ou sera commise [17] (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*) [18].

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, 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, respectivement, d'une amende maximale de 5 000 $ (nouvel art. 487.0197 du *Code*), ou 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*).

2.1.2.2 ORDONNANCES DE COMMUNICATION (ART. 13)

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 [19]. 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 [20]. La délivrance des ordonnances de communication spécifiques est basée sur le critère des motifs raisonnables de soupçonner.

L'article 13 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 FST [21] 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*) [22].

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 [23]. Ce type de données est utile, par exemple, pour retracer tous les FST qui ont participé à la transmission de données afin d'identifier le FST 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 la possession du FST 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*)[24]. 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[25] ou révèle des renseignements privilégiés[26]. 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*).

2.1.2.3 MANDAT POUR UN DISPOSITIF DE LOCALISATION (ART. 17)

À l'heure actuelle, l'article 492.1 du *Code* permet à un agent de la paix, muni d'un mandat[27], d'installer secrètement un « dispositif de localisation[28] » (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 17 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 (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*)[29].

2.1.2.4 MANDAT POUR UN ENREGISTREUR DE DONNÉES DE TRANSMISSION (ART. 17)

Actuellement, le paragraphe 492.2(1) du *Code* permet à un agent de la paix, muni d'un mandat [30], 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 17 du projet de loi prévoit un mandat qui autorise un agent de la paix à installer et activer un *enregistreur de données de transmission* [31] (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.

2.2 MODIFICATIONS À LA *LOI SUR LA CONCURRENCE*

2.2.1 ORDONNANCES DE PRÉSERVATION ET DE COMMUNICATION (ART. 20)

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 MODERNISATION DES INFRACTIONS (ART. 24 À 26)

Les articles 24 à 26 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 référence au *téléphone* comme moyen de commettre ces infractions par *tout moyen de télécommunication* utilisé pour communiquer oralement.

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 [32].

2.3.1 Perquisitions par le Commissaire de la concurrence (art. 28)

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*.

2.3.2 Ordonnances de communication (art. 32)

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. Ministère de la Justice du Canada, *Le gouvernement du Canada dépose un projet de loi pour lutter contre la criminalité dans un monde de haute technologie*, communiqué, 1er novembre 2010.
2. Pour plus de renseignements, voir Robin Mackay, *Résumé législatif du projet de loi C-54 : Loi sur la protection des enfants contre les prédateurs sexuels*, publication no 40-3-C54-F, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, Ottawa, 22 décembre 2010.
3. Pour plus de renseignements, 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-F, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, Ottawa, 9 novembre 2010. Le résumé législatif du projet de loi C-52 sera disponible bientôt.
4. Ministère de la Justice du Canada, Industrie Canada et Solliciteur général Canada, *Accès légal – document de consultation*, 25 août 2002.
5. Conseil de l'Europe, *Convention sur la cybercriminalité*, 23 novembre 2001, art. 16, 17 et 19.
6. *Ibid.*, art. 18.
7. Projet de loi C-52 : Loi régissant les installations de télécommunication aux fins de soutien aux enquêtes, 3e session, 40e législature.
8. Selon la définition actuelle qu'en donne le *Code criminel* [le *Code*] au par. 381(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.

9. Le terme « virus informatique » comprend aussi, dans le présent résumé législatif, les autres dispositifs malveillants, comme les vers informatiques.
10. *Code*, par. 430(1.1). Voir aussi l'art. 342.2.
11. *Convention sur la cybercriminalité*, art. 6.

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

13. La définition de « données informatiques » est donnée au par. 9(4) du projet de loi. Il s'agit essentiellement de données pouvant être traitées par ordinateur.

14. L'utilisation de l'expression « sa possession ou à sa disposition » dans le projet de loi fait en sorte que les FST devront probablement conserver, par suite d'un ordre ou d'une ordonnance, des données informatiques en plus de celles qu'ils recueillent dans le cadre normal de leurs activités commerciales.

15. 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.

16. 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*.

17. Cela inclut une infraction à la loi d'un État étranger.

18. 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*).

19. *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).

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

21. 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.

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

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

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

25. Une décision récente de la Cour suprême du Canada a jeté de la lumière sur la question de savoir si un FST devait être remboursé des coûts associés à l'exécution d'une ordonnance de communication pour produire des données d'appels téléphoniques. Selon la Cour, on devrait tenir compte de divers éléments, dont la portée de l'ordonnance demandée, la taille et la situation financière de la personne visée et l'ampleur des conséquences financières de la communication pour le FST (*Société Télé-Mobile* c. *Ontario*, [2008] 1 R.C.S. 305).

26. 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).

27. 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. 18 du projet de loi).

28. 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.

29. 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*).

30. Voir l'art. 487.11 du *Code* et l'art. 18 du projet de loi, qui n'exigent pas un mandat en situation d'urgence.

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

32. 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 ».