BIBLIOTHÈQUE du PARLEMENT
LIBRARY of PARLIAMENT

RÉSUMÉ LÉGISLATIF

Projet de loi C-13 :

Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle

Publication n^{o} 41-2-C13-F
Le 11 décembre 2013
Révisée le 28 août 2014

Julia Nicol
Dominique Valiquet

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

Les ***résumés législatifs*** de la Bibliothèque du Parlement, 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, qui effectue des recherches et prépare des informations et des analyses pour les parlementaires, les comités du Sénat et de la Chambre des communes et les 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**.

Résumé législatif du projet de loi C-13
(Résumé législatif)

Publication n^{o} 41-2-C13-F

This publication is also available in English.

TABLE DES MATIÈRES

RÉSUMÉ LÉGISLATIF DU PROJET DE LOI C-13 : LOI MODIFIANT LE CODE CRIMINEL, LA LOI SUR LA PREUVE AU CANADA, LA LOI SUR LA CONCURRENCE ET LA LOI SUR L'ENTRAIDE JURIDIQUE EN MATIÈRE CRIMINELLE

1 CONTEXTE

Le 20 novembre 2013, l'honorable Peter MacKay, ministre de la Justice, a présenté à la Chambre des communes le projet de loi C-13 : Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle (titre abrégé : « Loi sur la protection des Canadiens contre la cybercriminalité »).

1.1 OBJETS DU PROJET DE LOI ET PRINCIPALES MODIFICATIONS

Le projet de loi C-13 traite :

- de l'infraction de distribution non consensuelle d'images intimes;
- des infractions commises par tout moyen de télécommunication;
- d'un aspect de ce domaine du droit qu'on appelle en général « accès légal ».

L'accès légal est une technique d'enquête qui est employée par les organismes chargés de la sécurité nationale ou du contrôle d'application des lois et qui suppose l'interception de communications privées et la saisie d'information lorsque la loi l'autorise.

En matière d'accès légal, le projet de loi C-13 reprend essentiellement les dispositions de l'ancien projet de loi C-30 – déposé au cours de la première session de la 41e législature et mort au *Feuilleton* avant sa deuxième lecture à la Chambre des communes – à l'exception des dispositions concernant :

- la capacité d'interception des télécommunicateurs;
- la demande sans mandat de renseignements sur les abonnés[1].

Le 12 juin 2014, le Comité permanent de la justice et des droits de la personne de la Chambre des communes a amendé le projet de loi C-13 afin de prévoir un examen parlementaire des dispositions concernant l'accès légal.

Le projet de loi C-13 crée deux nouvelles infractions criminelles et vise à mettre à jour le droit pénal canadien. Plus précisément, les principales modifications apportées par le projet de loi consistent :

- à préciser que les infractions prévues au *Code criminel* (le *Code*) peuvent généralement être commises par tout moyen de télécommunication, et ce, pour que ces infractions puissent expressément s'appliquer à la cyberintimidation et aux autres activités criminelles qui ont lieu dans le cyberespace (art. 2);

- à créer une nouvelle infraction de distribution non consensuelle d'images intimes (art. 3);
- à instaurer l'ordonnance judiciaire interdisant d'utiliser un ordinateur ou Internet en cas de déclaration de culpabilité pour distribution non consensuelle d'images intimes (art. 3);
- à instaurer l'ordonnance judiciaire autorisant la saisie et la destruction d'images intimes (art. 4 et 5);
- à permettre, lorsqu'une autorisation d'interception de communications est accordée, la délivrance simultanée d'un mandat connexe, par exemple un mandat de perquisition (art. 8, 9 et 11);
- à élargir l'application des infractions d'encouragement au génocide et de propagande haineuse afin de protéger les personnes sur le fondement de l'origine nationale, de l'âge, du sexe ou de la déficience mentale ou physique (art. 12);
- à créer l'infraction de possession d'un virus informatique dans le but de commettre un méfait (art. 17);
- à donner aux organismes d'application de la loi la possibilité d'ordonner la préservation de preuves électroniques ou de l'obtenir par voie d'ordonnance judiciaire (art. 20);
- à créer de nouvelles ordonnances judiciaires de communication pour obtenir des données relatives à la transmission de communications, ou des données relatives à l'emplacement d'une chose ou d'une personne physique (art. 20);
- à créer des mandats afin 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. 23);
- à permettre le dédommagement de la personne qui a engagé des dépenses pour obtenir le retrait d'images intimes d'Internet (art. 24);
- à créer une ordonnance d'engagement pour prévenir la distribution d'images intimes (art. 25);
- à rendre habile à témoigner et contraignable le conjoint de la personne accusée de l'infraction de distribution non consensuelle d'images intimes (art. 27);
- à moderniser les infractions de pratiques commerciales trompeuses visées par la *Loi sur la concurrence* (art. 33 à 35);
- 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. 41).

1.2 CONTEXTE

1.2.1 CYBERINTIMIDATION

Le projet de loi porte en partie sur la cyberintimidation, sujet qui a fait les manchettes, particulièrement en raison des cas très médiatisés de Rehtaeh Parsons et d'Amanda Todd. Rehtaeh Parsons a fait une tentative de suicide en avril 2013

(ses appareils de maintien de la vie furent débranchés plus tard) après la diffusion d'images d'un viol allégué, situation qui a suscité diverses formes d'intimidation. Amanda Todd s'est suicidée en octobre 2012 après avoir été soumise à du chantage en ligne et menacée de voir diffuser sur Internet des photos d'elle la poitrine nue, une pratique surnommée « extorsion sexuelle ».

Également en octobre 2012, les ministres fédéraux, provinciaux et territoriaux responsables de la justice et de la sécurité publique ont demandé à leurs fonctionnaires d'examiner les lacunes éventuelles du *Code* en matière de cyberintimidation et de distribution non consensuelle d'images intimes. Le résultat de leur travail, *Cyberintimidation et distribution non consensuelle d'images intimes : Rapport aux ministres fédéraux/provinciaux/territoriaux responsables de la Justice et de la Sécurité publique*, a été publié en juin 2013 et comportait des recommandations qui ont été intégrées au projet de loi C-13[2].

En décembre 2012, le Comité sénatorial permanent des droits de la personne a publié un rapport sur la cyberintimidation, *La cyberintimidation, ça blesse! Respect des droits à l'ère numérique*, dans lequel il note :

> Malgré les différences d'opinions sur la nécessité de mettre à jour le *Code* en ce qui a trait à la cyberintimidation, la plupart des témoins ont tout de même affirmé clairement que, dans le cadre du travail auprès des jeunes, c'est l'approche de justice réparatrice qui est la plus efficace[3].

1.2.2 Obligations internationales en matière d'accès légal

En matière d'accès légal, le projet de loi C-13 représente une étape vers l'harmonisation des instruments qui permettent de lutter contre la cybercriminalité au Canada avec ceux d'autres pays, notamment en ce qui concerne les ordonnances de production et les ordonnances de préservation de données informatiques[4]. Le Canada a signé la *Convention sur la cybercriminalité* (la Convention) du Conseil de l'Europe en novembre 2001, ainsi que le Protocole additionnel sur les crimes haineux en juillet 2005[5]. La Convention dispose que les États parties au traité doivent créer des infractions aux termes de leurs lois internes pour criminaliser certains usages informatiques et qu'ils doivent adopter des mesures législatives adaptées aux nouvelles technologies, par exemple pour rendre des ordonnances de communication de « données relatives aux abonnés ».

2 DESCRIPTION ET ANALYSE

2.1 Modifications au *Code criminel*

2.1.1 La communication désigne également la télécommunication (art. 2)

L'article 2 du projet de loi modifie l'article 4 du *Code* pour préciser que lorsqu'une infraction comporte un élément de communication, celle-ci comprend les communications effectuées par tout moyen de télécommunication, à moins que le moyen soit précisé. Cela signifie clairement que, en règle générale, le fait qu'une infraction

soit commise au moyen d'un appareil de télécommunication n'est pas un obstacle à une condamnation[6].

2.1.2 DISTRIBUTION D'IMAGES INTIMES

2.1.2.1 NOUVELLE INFRACTION (ART. 3)

L'article 3 du projet de loi érige en infraction le fait pour quiconque de *sciemment* publier, distribuer, transmettre, vendre ou rendre accessible une « image intime » d'une personne, ou d'en faire la publicité. En vertu de cette disposition, qui se trouve dans le nouvel article 162.1 du *Code*, le fait de produire ou de posséder une image intime ou d'y accéder ne semble pas constituer un motif pour porter des accusations, contrairement à ce qui est le cas pour les infractions relatives à la pornographie juvénile énoncées à l'article 163.1 du *Code*.

Une « image intime » s'entend d'un enregistrement visuel (et non imprimé ou audio) – photographique, filmé, vidéo ou autre – d'une personne, dans lequel celle-ci répond à l'une ou l'autre des conditions suivantes :

- elle figure nue;
- elle expose ses seins, ses organes génitaux ou sa région anale;
- elle se livre à une activité sexuelle explicite.

En outre, pour qu'il y ait condamnation, il faut que la personne se trouve, *lors de la réalisation de cet enregistrement*, dans des circonstances pour lesquelles il existe une attente raisonnable de protection en matière de vie privée. La personne doit toujours avoir cette attente raisonnable de protection en matière de vie privée à l'égard de l'enregistrement *au moment de la perpétration de l'infraction* (p. ex. lorsque l'image est distribuée à autrui). Il reviendra aux tribunaux de déterminer ce qui constitue une attente raisonnable de protection en matière de vie privée dans le contexte de cette nouvelle disposition[7].

De même, la personne doit ne pas avoir consenti à la distribution de l'image ou l'accusé doit ne pas s'être soucié[8] de savoir si elle y a consenti ou non.

Enfin, nul ne peut être déclaré coupable de cette nouvelle infraction si les actes qui constitueraient l'infraction ont servi le bien public et n'ont pas outrepassé ce qui a servi celui-ci[9].

Il s'agit d'une infraction mixte pour laquelle le procureur peut choisir qu'elle soit punissable sur déclaration de culpabilité par mise en accusation ou par procédure sommaire. La mise en accusation peut mener à un emprisonnement maximal de cinq ans et la procédure sommaire, à une amende maximale de 5 000 $ et à une peine d'emprisonnement de six mois, ou à l'une de ces peines[10].

2.1.2.1.1 COMPARAISON AVEC LES INFRACTIONS RELATIVES À LA PORNOGRAPHIE JUVÉNILE ET AU VOYEURISME

La plupart des recommandations contenues dans le rapport Cyberintimidation et distribution non consensuelle d'images intimes : Rapport aux ministres fédéraux/provinciaux/territoriaux responsables de la Justice et de la Sécurité publique de juin 2013, préparé par le Groupe de travail du Comité de coordination des hauts fonctionnaires sur le cybercrime, ont été intégrées au projet de loi C-13. Le rapport signale que certains membres du Groupe de travail estimaient que les infractions relatives à la pornographie juvénile étaient un « instrument trop grossier » pour s'appliquer à la distribution non consensuelle d'images intimes, surtout lorsque l'accusé est un mineur. Ils ont fait la distinction entre l'atteinte à la protection de la vie privée et l'exploitation sexuelle d'enfants. Certains membres du Groupe de travail ont dit craindre que les accusations de pornographie juvénile puissent ne pas convenir dans certains cas. Ils estimaient que, si de telles accusations étaient portées, on pourrait être témoin de l'expansion involontaire des exceptions aux lois sur la pornographie juvénile[11]. La nouvelle infraction répond à ces préoccupations.

Par contre, le nouvel article 162.1 du *Code* sur les « images intimes » peut donner un résultat inattendu. Selon cette disposition, l'accusé ne peut être déclaré coupable si la personne présentée dans l'image a donné son consentement à la distribution, alors que le consentement n'est pas un moyen de défense sous le régime de l'article 163.1, qui traite de la pornographie juvénile. Cette différence peut donner lieu à la situation suivante si les images distribuées concernent un mineur :

- Si le mineur *a consenti* à la distribution, il est probable que l'auteur ne sera pas accusé en vertu du nouvel article 162.1, qui admet le consentement comme moyen de défense, mais plutôt en vertu de l'article 163.1, qui n'admet pas cette défense.
- Si le mineur *n'a pas consenti* à la distribution, l'auteur pourra être accusé en vertu de l'un ou l'autre des deux articles, puisque le consentement ne pourra pas être invoqué comme moyen de défense.

Puisque les sanctions sont plus lourdes en cas de pornographie juvénile et qu'elles comportent une peine minimale[12], l'accusé pourrait faire l'objet d'une peine plus dure s'il a obtenu le consentement du mineur que s'il ne l'a pas obtenu.

Il semble également que la nouvelle disposition ne prévoie pas de limite quant à l'âge à partir duquel un mineur peut consentir à la distribution d'une image intime. Le projet de loi n'ajoute pas la nouvelle infraction à l'article 150.1 du *Code*, qui énumère les infractions de nature sexuelle pour lesquelles le consentement de la victime ne constitue pas un moyen de défense, ainsi que les règles en matière d'âge de consentement.

La nudité de nature non sexuelle semble suffire pour satisfaire aux conditions de la nouvelle infraction[13]. Par contre, la nudité ne semble pas être un motif suffisant dans le cas des infractions relatives à la pornographie juvénile. Ces dernières comportent des expressions comme « dans un but sexuel » et « dont la caractéristique dominante est la représentation […] d'organes sexuels ». Malgré ces restrictions, la Cour

suprême du Canada a jugé nécessaire de préciser dans l'affaire *R. c. Sharpe* que les photographies de bébés nus et la nudité de nature non sexuelle ne sont pas visées par les infractions relatives à la pornographie juvénile[14].

Enfin, les dispositions du *Code* sur la pornographie juvénile font mention « d'organes sexuels ou de la région anale », tandis que la nouvelle infraction de distribution d'images intimes, ainsi que les articles 162 et 171.1 existants, utilise les termes « organes génitaux », « région anale » et « seins ». On ne sait pas bien si les termes employés sous-entendent autre chose. Il s'agit probablement d'allusions aux mêmes parties du corps, mais l'utilisation de termes distincts pourrait laisser croire que les significations sont différentes[15].

Le tableau 1 compare la nouvelle infraction aux infractions existantes de voyeurisme et de pornographie juvénile.

Tableau 1 – Comparaison du nouvel article 162.1 (distribution d'images intimes) et de dispositions existantes du *Code criminel*

Élément de l'infraction	Nouvel article 162.1 (distribution d'images intimes)	Article 162 (voyeurisme)	Article 163.1 (pornographie juvénile)
Type d'enregistrement	Enregistrement visuel – photographique, filmé, vidéo ou autre.	Enregistrement visuel – photographique, filmé, vidéo ou autre, réalisé par tout moyen[a].	Représentation photographique, filmée, vidéo ou autre représentation visuelle, réalisée ou non par des moyens mécaniques ou électroniques[b].
Contenu de l'image	La personne y figure nue, expose ses seins, ses organes génitaux ou sa région anale ou se livre à une activité sexuelle explicite.	La personne est nue, expose ses seins, ses organes génitaux ou sa région anale ou se livre à une activité sexuelle explicite[c].	Représentation, dans un but sexuel, d'organes sexuels ou de la région anale, ou d'une activité sexuelle explicite.
Une attente raisonnable de protection en matière de vie privée nécessaire pour une déclaration de culpabilité?	Oui	Oui	Non

Élément de l'infraction	Nouvel article 162.1 (distribution d'images intimes)	Article 162 (voyeurisme)	Article 163.1 (pornographie juvénile)
Types d'actes criminalisés	Sciemment publier, distribuer, transmettre, vendre ou rendre accessible l'enregistrement, ou en faire la publicité.	Effectuer, imprimer, copier, publier, distribuer, mettre en circulation, vendre ou rendre accessible un enregistrement ou en faire la publicité, ou l'avoir en sa possession en vue de faire une de ces actions.	163.1(2) : Produire, imprimer ou publier de la pornographie juvénile, ou en avoir en sa possession en vue de la publication. 163.1(3) : Transmettre, rendre accessible, distribuer, vendre, importer ou exporter de la pornographie juvénile ou en faire la publicité, ou en avoir en sa possession en vue de la transmettre, de la rendre accessible, de la distribuer, de la vendre, de l'exporter ou d'en faire la publicité. 163.1(4) : Avoir en sa possession de la pornographie juvénile. 163.1(4.1) : Accéder à de la pornographie juvénile.
Consentement	La personne n'a pas consenti ou l'accusé ne s'est pas soucié de savoir si elle a consenti ou non.	L'enregistrement doit se faire subrepticement.	Nul ne peut consentir à de la pornographie juvénile.
Âge de la personne dans l'enregistrement	Aucune condition d'âge.	Aucune condition d'âge.	Personne âgée de moins de 18 ans ou présentée comme telle et se livrant à une activité sexuelle explicite.
Peine maximale	Cinq ans sur déclaration de culpabilité par mise en accusation; 5 000 $ et six mois, ou l'une de ces peines, sur déclaration de culpabilité par procédure sommaire.	Cinq ans sur déclaration de culpabilité par mise en accusation; 5 000 $ et six mois, ou l'une de ces peines, sur déclaration de culpabilité par procédure sommaire.	163.1(2) et (3) : Dix ans avec minimum obligatoire d'un an sur déclaration de culpabilité par mise en accusation; deux ans moins un jour avec minimum obligatoire de six mois sur déclaration de culpabilité par procédure sommaire. 163.1(4) et (4.1) : Cinq ans avec minimum obligatoire de six mois sur déclaration de culpabilité par mise en accusation; 18 mois avec minimum obligatoire de 90 jours sur déclaration de culpabilité par procédure sommaire.
Versement de données dans la Banque nationale de données génétiques	Dans certains cas	Dans certains cas	Obligatoire[d].

Élément de l'infraction	Nouvel article 162.1 (distribution d'images intimes)	Article 162 (voyeurisme)	Article 163.1 (pornographie juvénile)
Inscription au registre des délinquants sexuels	Non	Dans certains cas[e].	Obligatoire[f].
Exceptions et moyens de défense	Si les actes qui constitueraient l'infraction ont servi le bien public et n'ont pas outrepassé ce qui a servi celui-ci.	Si les actes qui constitueraient l'infraction ont servi le bien public et n'ont pas outrepassé ce qui a servi celui-ci.	Si les actes qui constitueraient l'infraction ont un but légitime lié à l'administration de la justice, à la science, à la médecine, à l'éducation ou aux arts et ne posent pas de risque indu pour les personnes âgées de moins de 18 ans. Selon l'arrêt *R. c. Sharpe* : enregistrements privés d'activités sexuelles légales, conservés pour utilisation personnelle.

a. L'art. 162 du *Code* s'applique aussi à quiconque, subrepticement, observe, notamment par des moyens mécaniques ou électroniques, mais ce fait n'est pas pertinent pour la comparaison avec le nouvel art. 162.1.

b. L'art. 163.1 du *Code* s'applique aussi à tout écrit, à toute représentation ou à tout enregistrement sonore qui préconise ou conseille une activité sexuelle avec une personne âgée de moins de 18 ans, mais ce fait n'est pas pertinent pour la comparaison avec le nouvel art. 162.1.

c. Une infraction est commise même lorsque la personne n'est pas nue ou ne se livre pas à une activité sexuelle, mais que l'observation ou l'enregistrement est fait dans un but sexuel; voir le par. 162(1)*c*) du *Code*.

d. *Code*, art. 487.04 et par. 487.051(1).

e. *Ibid*., al. 490.011(1)*b*) et par. 490.012(2).

f. *Ibid*., al. 490.011(1)*a*) et par. 490.012(1).

2.1.3 ORDONNANCES RELATIVES AUX IMAGES INTIMES (ART. 4, 5 ET 7)

À l'heure actuelle, l'article 164 du *Code* permet à un juge de délivrer un mandat autorisant la saisie d'un enregistrement voyeuriste, d'une matière obscène, d'une histoire illustrée de crime[16] ou de toute matière qui constitue de la pornographie juvénile. Le juge peut aussi rendre une ordonnance la déclarant confisquée pour qu'il en soit disposé ou, s'il n'est pas convaincu qu'il s'agit de telle matière, exigeant qu'elle soit remise à la personne de laquelle elle a été saisie. L'article 4 du projet de loi ajoute les images intimes à cette liste, permettant ainsi aux tribunaux d'en ordonner la saisie et la confiscation. (Pour en savoir plus sur la confiscation, voir la partie 2.1.4.2 du présent résumé législatif.)

En outre, l'article 164.1 autorise le juge à ordonner au gardien de l'ordinateur dans lequel sont conservés un enregistrement voyeuriste, de la matière constituant de la pornographie juvénile ou les données afférentes :

- de remettre une copie électronique de la matière au tribunal;
- de s'assurer que la matière n'est plus emmagasinée ni accessible au moyen de l'ordinateur;
- de fournir les renseignements nécessaires pour identifier et trouver la personne qui a affiché la matière.

Cet article a été adopté pour autoriser la fermeture des sites Web comportant du matériel de pornographie juvénile ou voyeuriste. L'article 5 du projet de loi ajoute les images intimes à la liste des matières pour lesquelles un juge peut délivrer une ordonnance de saisie en vertu de l'article 164.1.

Enfin, l'article 7 du projet de loi ajoute l'infraction relative à la distribution non consensuelle d'images intimes à la liste de l'article 183 du *Code*, qui porte sur les infractions pour lesquelles peut être délivrée une autorisation judiciaire d'intercepter par voie électronique des communications privées. Cela signifie que les organismes d'application de la loi pourront utiliser la surveillance électronique pour enquêter sur cette nouvelle infraction.

2.1.4 Autres types d'ordonnance (art. 3, 6, 24 et 25)

Le projet de loi autorise le tribunal à délivrer certains types d'ordonnance pour répondre à diverses préoccupations concernant la distribution d'images intimes.

2.1.4.1 Ordonnance d'interdiction d'utiliser Internet (art. 3)

L'article 3 du projet de loi dispose que le tribunal qui inflige une peine ou prononce l'absolution conditionnelle du contrevenant reconnu coupable de l'infraction mentionnée au nouvel article 162.1 peut aussi rendre une ordonnance interdisant au contrevenant d'utiliser Internet ou tout autre réseau numérique, sauf en conformité avec les conditions imposées par le tribunal. L'interdiction peut être ordonnée pour la période que le tribunal juge appropriée, y compris la période d'emprisonnement à laquelle le contrevenant est condamné. L'omission de se conformer à l'ordonnance constitue une infraction mixte passible d'une peine d'emprisonnement maximale de deux ans.

2.1.4.2 Confiscation (art. 6)

L'article 164.2, dans son libellé actuel, autorise le tribunal qui déclare un accusé coupable d'une infraction visée à ordonner, sur demande du procureur général, la confiscation d'un bien, autre qu'un bien immeuble, qui a été utilisé pour commettre l'infraction et qui soit appartient à une personne qui a participé à l'infraction, soit a été transféré à autrui dans le but d'en éviter la confiscation. L'article 6 du projet de loi ajoute l'infraction mentionnée à l'article 162.1 à la liste des infractions auxquelles s'applique l'article 164.2.

2.1.4.3 Ordonnance de dédommagement (art. 24)

L'article 738 du *Code* autorise un tribunal à rendre une ordonnance de dédommagement dans certaines circonstances, par exemple lorsque le contrevenant a endommagé des biens ou que la victime a été forcée d'engager des dépenses pour, entre autres choses, rétablir son identité ou son dossier de crédit. L'article 24 du projet de loi permet au tribunal de rendre une ordonnance de dédommagement contre l'accusé reconnu coupable de l'infraction mentionnée au nouvel article 162.1 si la personne touchée a engagé des dépenses liées au retrait d'images intimes d'Internet ou de tout autre réseau numérique.

2.1.4.4 ENGAGEMENT DE NE PAS TROUBLER L'ORDRE PUBLIC (ART. 25)

L'article 25 du projet de loi ajoute un nouveau motif pour accorder, en vertu de l'article 810 du *Code*, un engagement de ne pas troubler l'ordre public lorsqu'une personne craint, pour des motifs raisonnables, qu'une autre personne commette l'infraction mentionnée au nouvel article 162.1.

2.1.5 TÉMOIGNAGE DU CONJOINT (ART. 27)

Selon la règle générale observée en common law, le conjoint d'une personne accusée n'est pas un témoin habile ni contraignable pour le poursuivant, hormis quelques exceptions énumérées[17] à l'article 4 de la *Loi sur la preuve au Canada*[18]. Le projet de loi modifie cette loi pour y ajouter une nouvelle exception afin que le conjoint d'une personne accusée d'avoir commis l'infraction visée au nouveau paragraphe 162.1(1) soit un témoin contraignable, ce qui signifie qu'il pourrait être obligé par le poursuivant à témoigner contre la personne accusée.

2.1.6 INTERCEPTION DE COMMUNICATIONS PRIVÉES (ART. 8 À 11)

La partie VI du *Code* (« Atteintes à la vie privée », art. 183 et suivants) est la pièce maîtresse de la législation canadienne en matière d'écoute électronique par les organismes d'application de la loi (« écoute électronique ») et s'applique à toutes les infractions énumérées à l'article 183 du *Code*. S'appliquant à l'interception du contenu d'une communication orale ou d'une séquence vidéo et impliquant souvent une intrusion importante dans la vie privée, la partie VI établit des conditions plus strictes pour la délivrance d'une autorisation judiciaire d'intercepter des communications privées que pour l'obtention d'un mandat de perquisition ou d'une ordonnance de communication[19].

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

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

Que l'interception se fasse avec le consentement de l'une des parties à la communication (art. 184.2 du *Code*), sans le consentement des parties (art. 185 et 186 du *Code*) ou pour une période maximale de 36 heures dans le cas d'une situation d'urgence (art. 188 du *Code*), le juge peut, en vertu du projet de loi, en plus d'accorder l'autorisation d'intercepter, délivrer un mandat de perquisition, un mandat général, une ordonnance de communication générale, une ordonnance de communication spécifique pour obtenir certaines informations (comme des données informatiques ou bancaires), une ordonnance d'assistance ou un mandat pour l'utilisation d'un dispositif de localisation ou d'un « enregistreur de données de

transmission » (art. 8, 9 et 11 du projet de loi). Dans tous les cas, ces articles du projet de loi visent à permettre aux policiers d'enquêter plus rapidement sur une infraction passée ou éventuelle.

Tous les documents relatifs à une demande d'autorisation d'intercepter des communications sont confidentiels; c'est pourquoi ils sont placés dans un paquet scellé par le juge (art. 187 du *Code*). L'article 10 du projet de loi précise que tous les documents relatifs aux demandes d'ordonnance ou de mandat connexes dans le contexte d'une autorisation seront aussi gardés secrets.

2.1.7 GÉNOCIDE ET PROPAGANDE HAINEUSE (ART. 12)

L'article 318 du *Code* criminalise le fait d'encourager le génocide à l'égard de certains « groupes identifiables » énumérés. À l'heure actuelle, « 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. L'article 12 du projet de loi ajoute à cette définition l'origine nationale, l'âge, le sexe et la déficience mentale ou physique. Étant donné que l'article 319, qui criminalise l'incitation publique à la haine (aussi appelée « propagande haineuse »), fait appel à la définition de « groupe identifiable » de l'article 318, le projet de loi criminalise également la propagande haineuse fondée sur l'origine nationale[20], l'âge, le sexe et la déficience mentale ou physique[21].

2.1.8 DISPOSITIF POUR VOLER DES SERVICES DE TÉLÉCOMMUNICATION (ART. 15)

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 15 du projet de loi ajoute essentiellement les infractions relatives à l'importation et à la mise à disposition d'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.

2.1.9 VIRUS INFORMATIQUE (ART. 17)

Selon les dispositions actuelles du *Code*, seules la propagation d'un virus informatique[22] ou la tentative de propagation constituent une infraction[23]. Conformément aux exigences de la *Convention sur la cybercriminalité*[24], l'article 17 du projet de loi rend illégales la possession d'un virus informatique en vue de commettre une infraction de méfait, ainsi que l'importation d'un tel virus et le fait de le rendre accessible.

2.1.10 COMMUNICATIONS FAUSSES, INDÉCENTES OU HARCELANTES (ART. 18)

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 » (terme utilisé actuellement au par. 372(3) du *Code* et que le projet de loi remplace par « harcelants ») font mention de certaines technologies de communication utilisées pour commettre ces infractions, comme le télégramme, la radio et le téléphone[25]. L'article 18 du projet

de loi modifie ces infractions en supprimant les mentions de ces technologies de communication particulières et, pour certaines de ces infractions, en y substituant la mention de « tout moyen de télécommunication ». Ainsi, des accusations de cyberintimidation, par exemple, pourront être déposées, peu importe le moyen de transmission ou la technologie utilisés.

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

2.1.11 ORDRE ET ORDONNANCE DE PRÉSERVATION (ART. 20)

Les renseignements sous forme électronique peuvent être détruits ou modifiés facilement et rapidement. L'article 20 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. L'ordre de préservation est donné par un agent de la paix (nouvel art. 487.012 du *Code*), tandis que l'ordonnance de préservation est rendue par un juge, sur demande d'un agent de la paix (nouvel art. 487.013 du *Code*).

L'ordre et l'ordonnance de préservation enjoignent à une personne, par exemple un télécommunicateur, de sauvegarder des « données informatiques[26] » qui sont « en sa possession ou à sa disposition » au moment où l'ordre ou l'ordonnance est reçu. Toutefois, un télécommunicateur peut toujours préserver *volontairement* des données et les communiquer *volontairement* à un organisme d'application de la loi, même en l'absence d'un ordre ou d'une ordonnance, sans s'exposer à des poursuites civiles ou criminelles (nouvel art. 487.0195 du *Code*)[27].

Ce nouvel outil d'enquête se distingue de la mesure de rétention des données en vigueur dans certains pays[28], qui contraint les télécommunicateurs à recueillir et à conserver des données pendant une période prescrite pour tous leurs abonnés, qu'ils fassent ou non l'objet d'une enquête. À l'opposé, l'ordre et l'ordonnance de préservation ne concernent qu'une télécommunication ou une personne en particulier, dans le cadre d'une enquête policière.

L'ordre ou l'ordonnance de préservation pourra être donné à un télécommunicateur uniquement s'il existe des « motifs raisonnables de soupçonner » qu'une infraction a été ou sera commise (nouveaux par. 487.012(2) et 487.013(2) du *Code*). Toutefois, la personne qui est soupçonnée de l'infraction ne peut être contrainte de conserver des données par suite d'un ordre ou d'une ordonnance de préservation (nouveaux par. 487.012(3) et 487.013(5) du *Code*). Il importe de signaler que le critère *motifs raisonnables de soupçonner* qu'une infraction a été ou sera commise est moins exigeant que le critère habituel, *motifs raisonnables de croire* qu'une infraction a été ou sera commise. Le critère *motifs raisonnables de soupçonner* est plus rare, mais il est déjà mentionné ailleurs dans le *Code*[29].

L'ordre et l'ordonnance de préservation sont des mesures temporaires, c'est-à-dire qu'ils sont généralement en vigueur juste assez longtemps pour permettre à l'organisme d'application de la loi d'obtenir un mandat de perquisition ou une ordonnance de communication. La durée maximale d'un ordre de préservation est de 21 jours (dans le cas d'une infraction à une loi fédérale) ou de 90 jours (dans le cas d'une infraction à une loi d'un État étranger) et l'ordre ne peut être donné qu'une seule fois (nouveaux par. 487.012(4) et (6) du *Code*), tandis que l'ordonnance de préservation a une durée de 90 jours et peut être renouvelée (nouveaux par. 487.013(6) et 487.194(2) du *Code*).

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

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

2.1.12 ORDONNANCES DE COMMUNICATION (ART. 20)

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[30]. 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 permettent d'obtenir certains renseignements précis : des informations bancaires ou des registres d'appels téléphoniques[31]. La délivrance des ordonnances de communication spécifiques est basée sur le critère moins exigeant des *motifs raisonnables de soupçonner* qu'une infraction a été ou sera commise.

L'article 20 du projet de loi crée de nouveaux types d'ordonnance de communication spécifique, dont la délivrance est basée sur l'existence de motifs raisonnables de soupçonner qu'une infraction a été ou sera commise. Elles permettent à un agent de la paix d'obtenir d'un télécommunicateur[32] 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*)[33].

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 son contenu[34]. Ce type de données est utile, par exemple, pour retracer tous les télécommunicateurs qui ont participé à la transmission de données afin d'identifier le télécommunicateur initial et ainsi déterminer l'origine d'une télécommunication (nouvel art. 487.015 du *Code*). Les « données de localisation » concernent l'emplacement d'une chose ou d'une personne physique.

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

Une procédure de révision est prévue pour contester tout type d'ordonnance de communication, existant et nouveau (nouvel art. 487.0193 du *Code*)[35]. 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[36] ou révèle des renseignements protégés[37]. Comme pour l'ordonnance de préservation, la violation d'une ordonnance de communication est punissable d'une amende maximale de 250 000 $ et d'une peine d'emprisonnement maximale de six mois, ou de l'une de ces peines (nouvel art. 487.0198 du *Code*).

2.1.13 EXAMEN PARLEMENTAIRE (ART. 20)

Le Comité permanent de la justice et des droits de la personne de la Chambre des communes a amendé le projet de loi afin d'ajouter le nouvel article 487.021 au *Code*. Cet article prévoit un examen parlementaire, dans les sept ans, des dispositions du projet de loi concernant les ordres et ordonnances de préservation ainsi que les ordonnances de communication, notamment l'immunité prévue au nouvel article 487.0195 du *Code*. La récente décision de la Cour suprême du Canada dans l'affaire *R. c. Spencer* contribuera probablement à l'interprétation de ce dernier article[38].

2.1.14 MANDAT POUR UN DISPOSITIF DE LOCALISATION (ART. 23)

À l'heure actuelle, l'article 492.1 du *Code* permet à un agent de la paix muni d'un mandat[39] d'installer secrètement un dispositif de localisation (p. ex. un dispositif GPS) sur une chose, s'il existe des motifs raisonnables de soupçonner qu'une infraction a été ou sera commise et s'il semble y avoir lieu de penser 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 23 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 un véhicule, 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*, par exemple un téléphone cellulaire, 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* qu'une infraction a été ou sera commise, 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 passe 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*)[40].

2.1.15 Mandat pour un enregistreur de données de transmission (art. 23)

Actuellement, le paragraphe 492.2(1) du *Code* permet à un agent de la paix muni d'un mandat de placer secrètement un enregistreur de numéro sur un téléphone ou une ligne téléphonique s'il existe des motifs raisonnables de soupçonner qu'une infraction a été ou sera commise et si 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 23 du projet de loi prévoit un mandat qui autorise un agent de la paix à installer et à activer un enregistreur de données de transmission[41] (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, comme le mandat pour placer un enregistreur de numéros téléphoniques, le nouveau mandat est basé sur le critère des motifs raisonnables de soupçonner qu'une infraction a été ou sera commise. Enfin, contrairement au projet de loi C-30, le projet de loi C-13 ne prévoit pas l'utilisation d'un enregistreur de données de transmission sans mandat en cas d'urgence.

2.2 Modifications à la *Loi sur la concurrence*

2.2.1 Ordonnances de préservation et de communication (art. 29)

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. 33 À 35)

Les articles 33 à 35 du projet de loi modernisent certaines infractions de pratiques commerciales trompeuses – par exemple donner de fausses indications sur un produit ou un service et le télémarketing trompeur – en remplaçant la mention du « téléphone » comme moyen de commettre ces infractions par celle de « tout moyen de télécommunication » utilisé pour communiquer oralement.

2.3 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 certains États en mettant en place un système d'échange de renseignements et d'éléments de preuve[42].

2.3.1 PERQUISITIONS PAR LE COMMISSAIRE DE LA CONCURRENCE (ART. 37)

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. 41)

Selon le projet de loi, les ordonnances de communication prévues par le *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.

2.4 ENTRÉE EN VIGUEUR (ART. 47)

L'article 47 prévoit que les dispositions du projet de loi C-13, à l'exception des dispositions de coordination, entreront en vigueur trois mois après la date à laquelle le projet de loi recevra la sanction royale.

NOTES

1. Pour plus d'informations sur ces questions, 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, sections 2.1.1 et 2.1.2.

2. Groupe de travail du Comité de coordination des hauts fonctionnaires sur le cybercrime, *Cyberintimidation et distribution non consensuelle d'images intimes – Rapport aux ministres fédéraux/provinciaux/territoriaux responsables de la Justice et de la Sécurité publique*, juin 2013.

3. Sénat, Comité permanent des droits de la personne, *La cyberintimidation, ça blesse! Respect des droits à l'ère numérique*, décembre 2012.

4. Pour plus de renseignements sur les lois d'autres pays en matière d'accès légal, voir Christopher Parsons, *Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm, and Future Canadian Policies*, 7 février 2012.

5. Conseil de l'Europe, *Convention sur la cybercriminalité*, 23 novembre 2001, Série des traités européens (STE) n^{o} 185, art. 18 (entrée en vigueur le 1er juillet 2004); Conseil de l'Europe, *Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, 28 janvier 2003, STE n^{o} 189 (entré en vigueur le 1er mars 2006).

6. La députée Hedy Fry a proposé des projets de loi qui auraient apporté les mêmes précisions au sujet de certaines infractions. Le plus récent d'entre eux, le projet de loi C-273, a été déposé pendant la 1re session de la 41^{e} législature.

7. Le même terme est employé à l'art. 162 (voyeurisme) du *Code criminel* (le *Code*); cet article pourrait être utile pour interpréter la disposition, mais il s'agit également d'une nouvelle disposition, adoptée en 2005, et la jurisprudence la concernant est assez limitée. On a jugé que le fait d'être nu ou de se livrer à des activités sexuelles dans une chambre à coucher, par exemple, pouvait donner lieu à une attente raisonnable de protection en matière de vie privée : voir *Regina v. Coombs*, 2013 ONSC 5243 (CanLII); *R. c. Larouche*, 2012 CM 3009 (CanLII); et *R. v. Keough*, 2011 ABQB 48 (CanLII) (peine modifiée en appel). Le tribunal a également jugé qu'il existait une attente raisonnable de protection en matière de vie privée dans un cas où un homme avait fait, à partir de son véhicule, un enregistrement vidéo de jeunes filles qui se trouvaient dans un parc : voir *R. v. Rudiger*, 2011 BCSC 1397 (CanLII). Il semble qu'aucune cour d'appel n'ait encore défini les limites de l'attente raisonnable de protection en matière de vie privée dans le contexte de l'art. 162.

8. Dans l'affaire *Sansregret c. la Reine*, la Cour suprême du Canada a défini l'insouciance comme « l'attitude de celui qui, conscient que sa conduite risque d'engendrer le résultat prohibé par le droit criminel, persiste néanmoins malgré ce risque. En d'autres termes, il s'agit de la conduite de celui qui voit le risque et prend une chance » (par. 16). Toutefois, dans l'affaire *Sansregret*, la Cour n'a pas établi le degré de risque nécessaire pour justifier une peine sous le régime du *Code*. En ce qui a trait au fait de conseiller une infraction qui n'est pas commise (art. 464 du *Code*), la Cour a établi ce seuil comme étant un « risque injustifié et important » (*R. c. Hamilton*, [2005] 2 R.C.S. 432, par. 29).

9. La même chose peut être dite au sujet des art. 162 (voyeurisme) et 163 (corruption des mœurs) du *Code*. Dans l'affaire *R. c. Sharpe*, [2001] 1 R.C.S. 45, la Cour suprême du Canada a discuté du moyen de défense fondé sur le bien public dans le contexte d'une accusation relative à la pornographie juvénile, une infraction pour laquelle ce moyen de défense existait à l'époque. Bien qu'elle n'ait pas procédé à une analyse complète, la Cour a donné quelques exemples d'utilisations pour le bien public qui pourraient s'appliquer à la distribution d'images intimes, notamment dans le cadre d'une poursuite en justice, ou encore pour une recherche sur les aspects politiques ou philosophiques de la question ou pour « l'épanouissement expressif ou psychologique ou qui renforce l'identité sexuelle d'une personne d'une façon non préjudiciable pour autrui » (par. 71).

10. La peine applicable sur déclaration de culpabilité par procédure sommaire est indiquée à l'art. 787 du *Code*, et non au nouvel art. 162.1.

11. L'affaire *R. c. Sharpe* a créé l'exception à l'art. 163.1 pour utilisation à des « fins personnelles » afin d'autoriser les enregistrements privés que font des adolescents de leurs activités sexuelles légales pourvu que de tels enregistrements soient utilisés à leurs fins personnelles.

12. L'infraction relative à la pornographie juvénile est une infraction mixte qui, sur déclaration de culpabilité par mise en accusation, est passible d'une peine d'emprisonnement maximale de cinq ans – ou dix ans – et d'une peine d'emprisonnement minimale obligatoire de six mois – ou un an – selon le paragraphe sous lequel l'accusation est déposée. La nouvelle infraction – également mixte – est passible, sur déclaration de culpabilité par mise en accusation, d'une peine d'emprisonnement maximale de cinq ans, mais d'aucune peine minimale obligatoire.

13. Cela pourrait inclure le fait de distribuer par courriel la photo d'un bébé nu à des grands-parents ou d'un érythème fessier à un médecin, par exemple, mais les tribunaux pourraient juger que le moyen de défense fondé sur le bien public s'applique à ces scénarios.

14. *R. c. Sharpe*, par. 73.

15. Le *Roget's International Thesaurus* (5e éd., Robert L. Chapman, HarperCollins Publishers, 1992), par exemple, donne « *sex organ* » (« organe sexuel ») comme un synonyme de « *genitals* » (« organes génitaux »), mais dit que les seins sont des caractéristiques sexuelles secondaires. On ne sait donc pas si les seins seraient inclus.

16. La définition d'« histoire illustrée de crime » est donnée au par. 163(7) du *Code*.

17. Voir *R. c. Hawkins*, [1996] 3 R.C.S. 1043, pour en savoir plus sur ce sujet.

18. Les tribunaux sont divisés quant à l'application de l'art. 4 de la *Loi sur la preuve au Canada* aux personnes vivant en concubinage. Par exemple, la Cour supérieure de justice de l'Ontario a déclaré que le fait d'appliquer la règle de common law sur l'incompétence des conjoints uniquement aux épouses et aux époux dont l'union est reconnue par une loi provinciale contrevient au par. 15(1) de la *Charte des droits et libertés* (*R. v. Edenlenbos*, (2000) 7 C.R.R. (2d) 154). Pour sa part, en 2009, la Cour d'appel de la Saskatchewan pensait le contraire lorsqu'elle a déclaré que ni la règle de common law sur l'incompétence des conjoints ni l'art. 4 ne s'appliquent aux personnes vivant en concubinage (*R. v. Martin* (2009), 64 C.R. (6th) 377).

19. Pour plus d'information sur les ordonnances de communication, voir la section 2.1.12 du présent résumé législatif.

20. La définition à l'art. 2 du *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* comprend également l'origine nationale. L'art. 20 du *Rapport explicatif* du Protocole se lit comme suit :

> La notion « d'origine nationale » doit être interprétée dans un large sens factuel. Il peut se référer à l'histoire d'une personne, non seulement quant à la nationalité ou l'origine de ses ancêtres, mais aussi par rapport à sa propre appartenance nationale, indépendamment du fait que cette personne possède ou non cette nationalité au sens juridique du terme. Lorsqu'une personne possède plusieurs nationalités ou est apatride, l'interprétation large de cette notion permet de la protéger si elle est discriminée sur la base de l'un de ces motifs. De plus, la notion « d'origine nationale » peut non seulement se référer à l'appartenance à un Pays qui est reconnu comme tel par la communauté internationale, mais aussi aux minorités ou à tout autre groupe de personnes avec des caractéristiques similaires.

21. Des dispositions distinctes s'appliquent à la propagande haineuse sous le régime de la *Loi canadienne sur les droits de la personne*, mais un projet de loi d'initiative parlementaire, le projet de loi C-304, les a abrogées en juin 2013, l'abrogation devant entrer en vigueur un an après cette date.

22. Dans le présent résumé législatif, le terme *virus informatique* comprend aussi d'autres dispositifs malveillants, comme les vers informatiques.

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

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

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

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

27. Le ministre fédéral de la Justice, Peter Mackay, a précisé que cette immunité n'est valable que si la communication volontaire s'est faite conformément aux dispositions de la loi, notamment la *Loi sur la protection des renseignements personnels et les documents électroniques* (voir le par. 7(3) de cette loi); voir Chambre des communes, Comité permanent de la justice et des droits de la personne, *Témoignages*, 28 novembre 2013.

28. Parlement européen, *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*, L 105/54.

29. Pour des exemples de l'utilisation des motifs raisonnables de soupçonner, voir le *Code* aux art. 83.3 (terrorisme), 254 (conduite avec capacités affaiblies), 487.13 (ordonnance de communication de données bancaires), 492.1 (mandat de localisation), 492.2 (mandat pour enregistreur de numéro) et 529.3 (pouvoir de pénétrer sans mandat en cas d'urgence). Pour une définition judiciaire des motifs raisonnables de soupçonner, voir *R. v. Cahil* (1992), 13 C.R. (4th) 327 (B.C. C.A.). Voir aussi la *Déclaration de la commissaire à la protection de la vie privée du Canada concernant le projet de loi C-13*, Ottawa, 28 novembre 2013.

30. *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).

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

32. 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.

33. Voir les définitions de ces types de données dans le nouvel art. 487.011 ajouté au *Code* par le projet de loi.

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

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

36. Dans un arrêt, la Cour suprême du Canada a répondu à la question de savoir s'il faut indemniser un télécommunicateur des coûts associés à l'obtempération à l'ordonnance de communication pour des relevés d'appels (art. 487.012 du *Code*). La Cour a jugé qu'il faut tenir compte de divers éléments, dont la portée de l'ordonnance demandée, la taille et la situation financière du télécommunicateur et l'ampleur des conséquences financières de la communication pour ce même télécommunicateur; voir *Société Télé-Mobile c. Ontario*, [2008] 1 R.C.S. 305.

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

38. *R. c. Spencer*, 2014 CSC 43. Dans cette décision, la Cour a conclu que la police doit être munie d'une ordonnance de communication pour contraindre un fournisseur de services Internet à lui divulguer le nom et l'adresse de la personne liée à une adresse IP. Interprétant l'actuel art. 487.014 du *Code* – qui est similaire au nouvel article 487.0195 prévu par le projet de loi C-13 – et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), la Cour a affirmé que :

> **ni le par. 487.014(1) du *C. Cr.*, ni la LPRPDE n'ont pour effet de conférer à la police des pouvoirs en matière de fouilles, de perquisitions ou de saisies [par. 71]**
>
> **Le paragraphe 487.014(1) est une disposition déclaratoire qui confirme les pouvoirs de common law permettant aux policiers de formuler des questions […] Puisque, en l'espèce, les policiers n'avaient pas le pouvoir d'effectuer une fouille ou une perquisition pour obtenir des renseignements relatifs à l'abonnée *en l'absence de circonstances contraignantes ou d'une loi qui n'a rien d'abusif*, je ne vois pas comment ils pourraient obtenir un nouveau pouvoir en matière de fouille ou de perquisition par l'effet combiné d'une disposition déclaratoire et d'une disposition adoptée afin de favoriser la protection des renseignements personnels [SOULIGNÉ PAR LES AUTEURS] [par. 73].**

39. S'il y a urgence et si 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; voir l'art. 487.11 du *Code* et aussi l'art. 26 du projet de loi.

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

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

42. Service des poursuites pénales du Canada, chapitre 43 : « L'entraide juridique en matière pénale », dans la partie VIII : « L'entraide internationale » du *Guide du Service fédéral des poursuites*.