THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Projet de loi C-13, *Loi sur la protection des Canadiens contre la cybercriminalité*

ASSOCIATION DU BARREAU CANADIEN

Mai 2014

500-865 Carling Avenue, Ottawa, ON, Canada K1S 5S8
tel/tél : 613.237.2925 | **toll free/sans frais** : 1.800.267.8860 | **fax/téléc** : 613.237.0185 | info@cba.org | **www.cba.org**

AVANT-PROPOS

L'Association du Barreau canadien est une association nationale qui regroupe 37 500 juristes, dont des avocats, des notaires, des professeurs de droit et des étudiants en droit dans l'ensemble du Canada. Les principaux objectifs de l'Association comprennent l'amélioration du droit et de l'administration de la justice.

Le présent mémoire a été préparé par la Section nationale du droit pénal, avec des commentaires de la Section nationale du droit à la vie privée, de la Section nationale du droit de la concurrence et du Comité du droit des enfants de l'Association du Barreau canadien, et avec l'aide de la Direction de la législation et de la réforme du droit du bureau national. Ce mémoire a été examiné par le Comité de la législation et de la réforme du droit et approuvé à titre de déclaration publique de l'Association du Barreau canadien.

TABLE DES MATIÈRES

Projet de loi C-13, *Loi sur la protection des Canadiens contre la cybercriminalité*

Projet de loi C-13, *Loi sur la protection des Canadiens contre la cybercriminalité*

I. INTRODUCTION

La Section nationale du droit pénal de l'Association du Barreau canadien, profitant de la participation de la Section nationale du droit de la vie privée, de la Section nationale du droit de la concurrence de l'ABC et du Comité du droit des enfants (ABC), est heureuse de formuler des commentaires sur le projet de loi C-13, *Loi sur la protection des Canadiens contre la cybercriminalité*. L'ABC reconnaît la nécessité de s'attaquer aux façons dont l'Internet peut être utilisé par certains pour harceler, intimider et menacer autrui, particulièrement les enfants vulnérables[1], activité qu'on appelle maintenant la cyberintimidation. Nous appuyons les efforts déployés par le gouvernement pour combler une « lacune » législative manifeste au moyen du projet de loi C-13 et faisons part de nos recommandations en vue de l'amélioration du projet de loi.

Le projet de loi C-13 criminalise la cyberintimidation, qui est devenue un problème de plus en plus urgent suivant une série d'affaires récentes et tragiques impliquant des adolescents intimidés en ligne. Les suicides tragiques de Rehtaeh Parsons et d'Amanda Todd, entre autres, ont déclenché un débat national.

Lorsqu'il a déposé le projet de loi C-13, l'honorable Peter MacKay, ministre de la Justice et Procureur général du Canada, a déclaré ce qui suit :

> Notre gouvernement est déterminé à protéger les enfants contre les prédateurs en ligne et l'exploitation en ligne. Nous avons le devoir d'aider à mettre fin au harcèlement et à l'exploitation nuisibles en ligne. La cyberintimidation s'étend bien au-delà de l'intimidation dans la cour d'école et, dans certains cas, elle peut devenir une activité criminelle[2].

---

1 Dans le présent mémoire, nous utilisons les termes « enfant » et « enfants » pour faire référence aux personnes âgées de moins de 18 ans qui ont des droits juridiques conférés par la *Convention des Nations Unies relative aux droits de l'enfant*, ratifiée par le Canada en 1991. Les termes « adolescent » et « adolescents » font référence plus particulièrement aux personnes ayant entre 12 et 17 ans, qui sont susceptibles de poursuites en vertu de la *Loi sur le système de justice pénale pour les adolescents*.

2 Ministère de la Justice, « Le gouvernement dépose un projet de loi pour sévir contre la cyberintimidation », http://www.justice.gc.ca/fra/nouv-news/nr-cp/2013/doc_32994.html.

L'ABC appuie l'objectif de protéger les enfants contre la cyberintimidation. Toutefois, le mécanisme servant à la réalisation de cet objectif – la création d'une nouvelle infraction criminelle – doit être rédigé avec précision pour englober seulement le comportement reproché. À cette fin, nous recommandons des modifications particulières à la disposition constitutive de l'infraction.

Le projet de loi C-13 va bien au-delà de la cyberintimidation et révise les dispositions générales applicables à la fouille et à la saisie de données Internet, ce qu'on appelle les dispositions sur « l'accès légal ». Les propositions que renferme le projet de loi C-13 sont plus ciblées et circonscrites que les initiatives législatives antérieures, et nous estimons que si nos modifications recommandées sont appliquées, cela produira une version viable de cet important projet de loi. Des dispositions mises à jour applicables à la fouille et la saisie de données Internet sont essentielles pour l'application de dispositions substantielles de droit pénal comme la nouvelle infraction de cyberintimidation.

Toutefois, d'anciens projets de loi sur l'accès légal ont été très controversés et, comme les dispositions sur l'accès légal contenues dans le projet de loi C-13, de telles dispositions peuvent détourner l'attention de la cyberintimidation. Pour que la protection des enfants et des adolescents reçoive l'attention qui leur est due, l'ABC propose de diviser le projet de loi C-13 en deux projets de loi distincts, soit l'un concernant la cyberintimidation et l'autre concernant l'accès légal.

RECOMMANDATION :

1. **L'Association du Barreau canadien recommande la division du projet de loi C-13 en deux projets de loi distincts, séparant les dispositions sur l'accès légal des nouvelles mesures visant expressément la cyberintimidation.**

II. L'INFRACTION DE CYBERINTIMIDATION

A. Combler la lacune

Le projet de loi C-13 introduit une infraction hybride visant à criminaliser la publication d'images intimes sans consentement :

> 162.1 (1) Quiconque sciemment publie, distribue, transmet, vend ou rend accessible une image intime d'une personne, ou en fait la publicité, sachant que cette personne n'y a pas consenti ou sans se soucier de savoir si elle y a consenti ou non, est coupable…

L'expression « image intime » est définie ainsi au paragraphe (2) :

> … un enregistrement visuel –photographique, filmé, vidéo ou autre – d'une personne, réalisé par tous moyens, ou celle-ci :
>
> a) y figure nue exposant ses seins, ses organes génitaux ou sa région anale ou se livrant à une activité sexuelle explicite;
>
> b) se trouvait, lors de la réalisation de cet enregistrement, dans des circonstances pour lesquelles il existe une attente raisonnable de protection en matière de vie privée;
>
> c) a toujours cette attente raisonnable de protection en matière de vie privée à l'égard de l'enregistrement au moment de la perpétration de l'infraction.

S'il est poursuivi par voie de mise en accusation, l'accusé est passible d'une peine d'emprisonnement maximale de cinq ans.

Comme l'illustrent les commentaires du ministre MacKay, le projet de loi C-13 vise avant tout à protéger les enfants et les adolescents contre les prédateurs et l'exploitation en ligne. Toutefois, les dispositions actuelles du *Code criminel* criminalisent déjà la diffusion de représentations sexuelles d'enfants (voir l'article 163.1 – pornographie juvénile). En fait, le libellé de la disposition proposée de cyberintimidation reflète les dispositions constitutives d'infractions de pornographie juvénile figurant au *Code criminel* et ces dernières dispositions procurent une plus grande protection que ne le fait le projet de loi C-13 car elles criminalisent la simple possession de telles images.

Ainsi, le véritable changement et l'élargissement des pouvoirs criminels prévu par le projet de loi C-13 portent sur l'utilisation illégale d'« images intimes » impliquant des adultes. À l'heure actuelle, les poursuivants doivent recourir à des dispositions constitutives d'infractions qui ont été adoptées avant l'existence de la cyberintimidation, comme la disposition constitutive de l'infraction de harcèlement criminel. Plutôt que d'augmenter la protection des enfants et des adolescents, cet aspect du projet de loi C-13 comble une lacune actuelle du régime législatif canadien.

En vertu du projet de paragraphe 162.1(1), quiconque publie, distribue, transmet, vend ou rend accessibles des images intimes d'adultes ou en fait la publicité sans consentement peut être inculpé. Compte tenu du préjudice grave que ce comportement peut causer, l'ABC se réjouit de cet ajout au *Code criminel*, encore une fois sous réserve des améliorations recommandées ci-après.

Le projet de loi C-13 n'augmente pas en réalité la protection des enfants et des adolescents victimes de cyberintimidation, mais la disposition proposant l'infraction offrirait aux poursuivants une importante solution de rechange lorsqu'ils ont affaire à des personnes âgées de moins de 18 ans qui auraient diffusé des images intimes d'autres adolescents. Le projet de loi prévoit une possibilité plus modérée de poursuite des adolescents qui diffusent des images intimes de leurs pairs sans consentement que les dispositions actuelles en matière de pornographie juvénile, dont les sanctions et les stigmates connexes sont plus durs.

Manifestement, la cyberintimidation constitue un problème grave pour les enfants et les adolescents au Canada. Toutefois, le droit criminel devrait être considéré comme un outil de dernier recours lorsqu'il est question de jeunes délinquants, et les incidents de cyberintimidation de la part d'adolescents ne devraient pas tous être qualifiés d'actes criminels. Pour la plupart des jeunes délinquants, une intervention éducative ou de déjudiciarisation convient mieux[3]. Il est aussi important de reconnaître que les adolescents sont souvent non seulement des victimes, mais peuvent eux-mêmes être des « cyberintimidateurs » ou des « spectateurs » à d'autres moments. Il faut analyser minutieusement cet élément pour déterminer ce qui est vraiment dans l'intérêt supérieur de tous les enfants canadiens, car ces rôles peuvent changer d'une interaction à l'autre.

B. « Publie, distribue, transmet, vend ou rend accessible une image intime ou en fait la publicité »

Le projet d'article 162.1 englobe divers types de cyberintimidation, criminalisant certains actes qui ne sont pas actuellement interdits et, encore une fois, visant d'autres actes déjà qualifiés de pornographie juvénile à l'article 163.1 du *Code criminel*. Le projet d'article 162.1 criminalise toute diffusion d'images intimes sans le consentement de la personne représentée. Toutefois, de la façon dont elle est rédigée, la disposition s'applique également aux comportements qui ne seraient pas généralement considérés comme de la cyberintimidation.

La fiche d'information, le communiqué et les commentaires ministériels relatifs au projet de loi C-13 indiquent tous que ce projet de loi luttera contre la distribution illégale d'images intimes en vue de l'intimidation des personnes représentées dans les images. L'intimidation

---

[3] Pour consulter une analyse utile des mesures de rechange non pénales adoptées pour lutter contre la cyberintimidation, veuillez consulter : Groupe de travail du Comité de coordination des hauts fonctionnaires sur le cybercrime, « Rapport aux ministres fédéraux/provinciaux/territoriaux responsables de la Justice et de la Sécurité publique : Cyberintimidation et distribution non consensuelle d'images intimes », juin 2013 [Groupe de travail des CCHF sur le cybercrime] aux pages 6 à 8.

peut emprunter de nombreuses formes, y compris le harcèlement, l'embarras, la contrariété et l'intimidation. L'intimidation est délibérée. Nous présumons que le projet de loi ne vise pas à englober la distribution par inadvertance ou inattention d'images, sans le mobile ou l'intention nécessaire, mais le libellé actuel de l'article 162.1 pourrait avoir cet effet[4].

Même si les dispositions relatives à la cyberintimidation visent expressément à criminaliser le comportement entaché d'une intention malveillante, elles englobent le comportement non accompagné d'une telle intention. Le libellé proposé de l'article 162.1 est compatible avec une disposition constitutive d'infraction relative à la vie privée, comme le recommandait le Groupe de travail du Comité de coordination des hauts fonctionnaires (CCHF) sur le cybercrime[5]. Toutefois, l'intention exprimée par le législateur en ce qui a trait au projet de loi C-13 consiste à criminaliser la cyberintimidation, définie comme « l'utilisation des technologies de l'information et des communications qui facilitent le comportement délibéré, hostile et souvent répété d'une personne ou d'un groupe *dans l'intention de faire du mal à d'autres* »[6]. L'ABC estime que le libellé de la disposition devrait être peaufiné de manière à se conformer à son objet déclaré.

Par exemple, l'expression « rend accessible » figurant au projet d'article 162.1 crée des possibilités de responsabilité criminelle allant bien au-delà de ce que les Canadiens raisonnables considéreraient comme de la cyberintimidation. Prenons l'exemple suivant :

> M. Smith prête son ordinateur portatif à un ami, M. Jones, pour que celui-ci navigue sur Internet pendant que son câble est réparé. M. Smith sait que l'ordinateur contient deux images intimes de lui-même et de son épouse, mais ces images se trouvent bien enfouies dans un dossier appelé « Personnel ». M. Smith sait également que son épouse s'attend à ce que ces images demeurent privées. Il est convaincu que M. Jones n'explorera pas l'ordinateur pour examiner chaque dossier.
>
> Toutefois, M. Jones devient las de naviguer sur Internet et commence à ouvrir des dossiers au hasard – découvrant finalement les deux images intimes. En même temps, une personne lui rendant visite chez lui, aussi une connaissance de l'épouse

---

4 Il n'est pas rare pour des adolescents de prendre des photos sexuellement explicites d'eux-mêmes en vue de les partager avec d'autres adolescents qui, de leur côté, peuvent distribuer les images sans consentement. Poursuivre des adolescents pour des infractions de pornographie juvénile dans ces circonstances va vraisemblablement au-delà de l'esprit de l'article 163.1 (voir *R. c. Sharpe*, [2001] 1 R.C.S. 45). Il y a actuellement une contestation constitutionnelle des dispositions relatives à la pornographie juvénile dans leur application aux adolescents dans des circonstances similaires. Cela fait ressortir l'importance de limiter la nouvelle infraction de cyberintimidation à la distribution non consensuelle d'images intimes.

5 *Précité*, note 3.

6 *Ibid.* à la p. 3.

de M. Smith, passe par là et voit l'image. Troublée, elle en informe la police et l'ordinateur est saisi.

Dans cet exemple, M. Smith n'a pas l'intention d'intimider son épouse en prêtant son ordinateur portatif à son ami. En vertu du projet de loi C-13, il pourrait être déclaré coupable d'« avoir rendu accessible une image intime sans le consentement », puisqu'il a intentionnellement rendu accessible son ordinateur à M. Jones en sachant que des images intimes s'y trouvaient et que son épouse n'avait pas consenti à les partager.

Il est facile d'imaginer d'autres exemples dans lesquels une personne aurait rendu des images intimes accessibles sans avoir l'intention d'intimider les gens représentés dans les images. On peut créer des hyperliens à pratiquement n'importe quoi sur Internet, de sorte que la possibilité de « rendre accessible » des images est illimitée.

Le projet de loi C-13 pourrait aussi avoir un effet sur les médias. Il semble que les photojournalistes qui publient des images de personnes célèbres ou de politiciens se trouvant en situation compromettante pourraient être passibles de sanctions criminelles en vertu du projet de loi[7].

De simples ajouts à l'article 162.1 pourraient régler ce problème et en restreindre la portée aux comportements que le législateur envisage apparemment – l'intimidation intentionnelle d'autrui au moyen de la diffusion d'images intimes.

RECOMMANDATION :

2. **L'Association du Barreau canadien recommande la modification du paragraphe 162.1(1) par l'ajout des mots « avec l'intention de contrarier, d'embarrasser, d'intimider ou de harceler cette personne ».**

3. **L'Association du Barreau canadien recommande l'ajout suivant à l'article 162.1 : « Nul ne peut être déclaré coupable d'une infraction en vertu du présent article si la distribution, la transmission, la vente, le fait de rendre accessible ou la publicité qui constitue l'objet de l'accusation est destiné à l'information du public ou constitue une question d'intérêt public ».**

---

7 Le projet de loi prévoit une défense du « bien public » qui pourrait éliminer en partie le risque que les médias se fassent poursuivre au criminel.

C. L'insouciance et la connaissance concernant le consentement

Si une personne prend ou reçoit une image intime directement d'une connaissance personnelle, il peut être facile de déterminer si le consentement à la communication ultérieure de l'image a été donné. Toutefois, les ordinateurs portatifs, les téléphones intelligents et les autres dispositifs électroniques facilitent la communication et le transfert d'images intimes à plusieurs reprises en quelques secondes seulement. Cela donne à penser qu'il y a une échelle mobile de culpabilité morale et une vaste gamme de personnes qui pourraient être accusées de l'infraction proposée, dont certaines ne connaissent pas ou connaissent peu la personne représentée dans l'image.

L'inclusion de l'« insouciance » dans l'infraction proposée soulève la question de savoir s'il faut prendre des mesures pour vérifier le consentement avant de communiquer une image, même si on ne connaît pas la personne représentée ou la façon dont l'image a été obtenue. Dans de telles circonstances, il sera souvent impossible de vérifier l'existence du consentement.

Nous le répétons, la disposition proposée vise à criminaliser la communication d'une image en vue d'intimider la personne qui y est représentée. Si on distribue une image intime sans connaître sa provenance ou la personne représentée, on n'a pas l'intention d'intimider la personne représentée. Toutefois, selon la formulation actuelle de la disposition, la personne qui communique l'image pourrait faire l'objet de sanctions criminelles si elle fait preuve d'insouciance quant à la question de savoir si le consentement a été obtenu.

L'élimination de la norme d'insouciance du projet de disposition constitutive d'infraction rétablirait l'accent que l'on veut mettre sur ce qui constitue vraiment de la cyberintimidation. Cela reflète la distinction fondamentale entre les dispositions qui visent à lutter contre l'intimidation et les dispositions qui visent simplement à protéger la vie privée.

Le projet d'article 162.2 devrait reposer sur le mot « sciemment. » En droit criminel, la notion de connaissance englobe le concept d'« aveuglement volontaire ». La norme de l'aveuglement volontaire s'applique aux délinquants qui savent qu'ils doivent s'informer du consentement, mais refusent de le faire (parce qu'ils ne veulent pas savoir s'il y a consentement)[8]. En d'autres termes, même sans la norme d'insouciance, l'accusé peut être déclaré coupable s'il soupçonnait

8 *R. c. Sansregret*, [1985] 1 R.C.S. 570.

l'absence de consentement, mais ne s'en est pas soucié à dessein avant de communiquer l'image intime.

Dans l'exemple précédent, si M. Jones avait par la suite copié les images intimes qu'il a trouvées et les avaient envoyées par courriel à un autre ami (M. Johnson), il serait responsable en vertu de l'article 162.1 même s'il n'a pas personnellement pris les photos et ne les a pas demandées à M. Smith. Compte tenu de la nature des images, du fait que M. Jones connaissait la personne représentée et du fait qu'il a trouvé les images parmi plusieurs dossiers, dans un dossier nommé « Personnel », il a vraisemblablement fait preuve d'aveuglement volontaire quant à la question du consentement.

Mais supposons que M. Johnson ait reçu les images inattendues et bouleversantes sur son téléphone pendant qu'il se trouvait à côté d'un ami et qu'il les a montrés à cet ami. Il ignorait la personne figurant dans les images, l'endroit où elles avaient été prises et le nom du dossier dans lequel elles avaient été trouvées. Pourtant, si M. Johnson savait qu'il se pouvait que les personnes représentées dans les images n'aient pas consenti à la distribution (p. ex., en raison du caractère amateur de la photo[9]), il pourrait être considéré insouciant quant au consentement du fait qu'il a réagi instinctivement en se tournant vers son ami pour lui montrer les images. Selon la formulation actuelle du projet de loi C-13, M. Johnson pourrait être tenu criminellement responsable sans avoir eu l'intention d'intimider l'épouse de M. Smith (ou M. Smith.). La « distribution » par M. Johnson des images (lorsqu'il s'est retourné vers son ami pour lui montrer son téléphone) ne semble pas relever des comportements que le projet de loi C-13 vise à criminaliser.

RECOMMANDATION :

4. **L'Association du Barreau canadien recommande la modification du paragraphe 162.1(1) de manière à supprimer les mots « ou sans se soucier de savoir si elle y a consenti ou non ».**

---

9 Par ailleurs, si une photo ne semble pas être le fait d'un amateur, mais semble plutôt avoir été prise par un professionnel, le destinataire peut raisonnablement présumer que la personne qui pose est une professionnelle et ne pas songer à l'existence d'un problème de consentement ou d'intimidation. La poursuite pour distribution ne devrait pas dépendre de lacunes manifestes d'une photo, de la qualité de la caméra, etc.

D. Les fournisseurs de plateformes neutres

Le projet de loi C-13 pourrait criminaliser les plateformes Internet conçues pour le partage légal de contenu, conformément à des « conditions d'utilisation », à des « normes de la collectivité » ou à d'autres règles de conduite. Malgré de telles précautions, les fournisseurs de plateformes neutres pourraient contribuer sans le vouloir à la cyberintimidation.

Les fournisseurs de services en ligne ne connaissent pas le matériel stocké sur leurs plateformes ou ce qui est communiqué aux autres utilisateurs et ne devraient pas risquer la responsabilité criminelle en raison du comportement de leurs utilisateurs sauf s'ils sont aussi coupables. Par exemple, certains sites Web de médias sociaux permettent à un utilisateur de « partager » une image avec un petit groupe d'utilisateurs ou avec le grand public. Le fournisseur de site Web pourrait être incapable d'examiner les images à l'avance et ignorer si la personne représentée dans une image a consenti à la diffusion de cette image. Les sociétés de télécommunications qui fournissent des services de messages textes ou de messages vidéos se trouvent dans la même situation. Si la culpabilité est fondée sur l'« insouciance », ce qui crée une obligation de se renseigner, les fournisseurs de plateformes seront vraisemblablement incapables d'identifier et de contacter les personnes qui figurent dans les images afin de s'informer de leur consentement.

Constitue un autre type de fournisseur de services neutre le moteur de recherche qui indexe le contenu disponible sur d'autres sites Web et services et produit des résultats en réponse à des demandes de recherche. Les exploitants de moteurs de recherche ignorent les circonstances dans lesquelles les images ou vidéos indexées ont été produites ou si les personnes ont consenti à leur diffusion. Il est peut-être impossible de trouver cette information à partir des images ou des données environnantes.

Certaines organisations en ligne existent en vue de diffuser des images intimes sans le consentement des personnes représentées. Ces organisations sont visées à juste titre par le projet de loi. Mais rendre criminellement responsables les fournisseurs de services neutres est déraisonnable et ne résisterait vraisemblablement pas à un examen fondé sur la *Charte* en raison de l'absence de culpabilité morale, ce qui est nécessaire pour l'imposition de sanctions criminelles.

RECOMMANDATION :

5. **L'Association du Barreau canadien recommande l'ajout suivant à l'article 162.1 : « Nul fournisseur de services de télécommunications, d'information, d'outils de localisation ou de réseau ne peut être déclaré coupable d'une infraction aux termes du présent article sauf s'il demande ou conseille à une autre personne de commettre une infraction visée par le présent article, l'y incite ou l'y invite, que cette autre personne commette ou non l'infraction.**

E. La peine

Une peine d'emprisonnement maximale de cinq ans s'inscrit dans une échelle appropriée de sanctions pour l'infraction constituée par le projet d'article 162.1. Cette peine maximale est conforme à des dispositions similaires du *Code criminel* et permet aux juges canadiens de statuer sur cette infraction au moyen d'une absolution sous conditions ou d'une peine d'emprisonnement avec sursis dans les cas qui s'y prêtent.

Le projet de loi C-13 modifierait également la disposition de restitution du *Code criminel* en ajoutant l'alinéa suivant :

> 738(1)*e*) dans le cas de la perpétration d'une infraction prévue au paragraphe 162.1(1), de verser à la personne qui, du fait de l'infraction, a engagé des dépenses raisonnables liées au retrait d'images intimes de l'Internet ou de tout autre réseau numérique des dommages-intérêts non supérieurs à ces dépenses si ces dommages peuvent être facilement déterminés.

L'ABC estime qu'il s'agit d'une modification logique et positive car elle vise à indemniser les victimes pour les coûts directs qu'elles engagent par suite de la cyberintimidation criminelle.

Enfin, le projet de loi C-13 propose une nouvelle ordonnance d'interdiction à l'article 162.2 :

> 162.2(1) Dans le cas où un contrevenant est condamné, ou absous en vertu de l'article 730 aux conditions prévues dans une ordonnance de probation, d'une infraction mentionnée au paragraphe 162.1(1), le tribunal qui lui inflige une peine ou prononce son absolution, en plus de toute autre peine ou de toute autre condition de l'ordonnance d'absolution applicables en l'espèce, sous réserve des conditions ou exemptions qu'il indique, peut interdire au contrevenant d'utiliser Internet ou tout autre réseau numérique, à moins de le faire en conformité avec les conditions imposées par le tribunal.

> (2) L'interdiction peut être ordonnée pour la période que le tribunal juge appropriée, y compris pour la période d'emprisonnement à laquelle le contrevenant est condamné.

Le paragraphe (3) permet la présentation d'une demande de modification d'une ordonnance rendue en vertu du paragraphe 162.2(1). Le paragraphe (4) constitue en infraction le défaut de se conformer à une ordonnance rendue en vertu du paragraphe 162.2(1). Il convient assurément dans certains cas d'interdire à un contrevenant d'avoir accès à l'Internet pendant un certain temps. Toutefois, le paragraphe 162.2(2) devrait être raisonnable et limité à un maximum de cinq ans. Selon sa formulation actuelle, le projet de loi permet au tribunal d'interdire l'utilisation de l'Internet à perpétuité. Compte tenu de l'omniprésence de l'Internet dans le fonctionnement quotidien de la société, cela pourrait être dévastateur et constituer une sanction disproportionnée.

La personne à qui on interdit d'accéder à l'Internet risque de ne pas pouvoir solliciter d'emploi en ligne (méthode de plus en plus courante de recrutement), payer ses factures en ligne, produire ses déclarations de revenus en ligne ou accomplir de nombreuses autres tâches essentielles qui, de plus en plus, ne peuvent être accomplies que par Internet. Les adolescents à qui on interdit d'avoir accès à l'Internet peuvent se voir empêcher de participer à des travaux et activités scolaires réguliers et ne pas pouvoir terminer leurs études. Le libellé actuel du paragraphe 162.2(1) comprend l'expression « à moins de le faire en conformité avec les conditions imposées par le tribunal », mais la disposition semble permettre au tribunal d'interdire à l'accusé d'accéder à l'Internet sans exception.

RECOMMANDATION :

6. **L'Association du Barreau canadien recommande la modification de l'article 162.2 de manière à obliger le tribunal à permettre au contrevenant de se prévaloir d'une ou de plusieurs exceptions à l'interdiction ordonnée en vertu du paragraphe 162.2(1).**
7. **L'Association du Barreau canadien recommande la modification du paragraphe 162.2(2) de manière à exiger une interdiction raisonnable, la période d'interdiction maximale d'accès à l'Internet devant se limiter à cinq ans.**

F. Conclusion

Toute mesure législative en réponse au problème social général de l'intimidation devrait s'accompagner d'une forte insistance sur l'éducation et la prévention de manière à ce que les adolescents – qu'il s'agisse des intimidateurs, des victimes ou des spectateurs potentiels ou réels – comprennent les conséquences sociales et juridiques et en matière de santé de leurs actes numériques pour eux et les autres. Les adolescents sont mieux en mesure de se protéger et de protéger les autres, et d'adapter leur comportement, lorsqu'ils sont efficacement informés des risques que constituent les courriels, les textes et les images non désirés et disposent d'outils pour y répondre.

Les adolescents sont non seulement plus impulsifs en raison de leur stade de développement, mais ils pensent moins à l'avenir que les adultes. Les intérêts à court terme l'emporteront vraisemblablement sur la possibilité apparemment lointaine de conséquences juridiques. Si on met trop l'accent sur les sanctions, plutôt que d'insister sur la prévention et l'éducation, on manque le moment où il faut s'attaquer au comportement – c.-à-d., avant qu'une personne, de façon impulsive, prenne une photo ou presse le bouton « Envoyer ». Seules les affaires les plus graves devraient donner lieu à des accusations criminelles contre des adolescents. Et il devrait y avoir une analyse et une évaluation continues et minutieuses des effets prévus et imprévus de ce projet de loi.

Dans le récent « bulletin » récemment décerné par l'UNICEF sur le bien-être des enfants, le Canada s'est classé au 21e rang sur 29 pays industrialisés quant à l'incidence de l'intimidation[10]. Les Canadiens devraient examiner la façon dont les pays se classant à un rang supérieur comme l'Italie, la Suède et l'Espagne préviennent les torts, les pertes et les décès inutiles. En définitive, il n'y a pas de « remède miracle » à la cyberintimidation et aux torts qu'elle cause – même en cas de sanctions criminelles. Un sens accru des responsabilités collectives peut faire une différence importante, les parents, enseignants, travailleurs sociaux, professionnels de la santé, agents d'application de la loi, décideurs et le secteur privé, avec les adolescents, jouant tous un rôle plus important dans la prévention efficace et dans la communication sensible.

10 www.unicef.org/policyanalysis/index_68637.html

III. L'ACCÈS LÉGAL

A. Introduction : Le respect de la vie privée et l'application de la loi

Au cours des douze dernières années, l'ABC a formulé des commentaires sur plusieurs propositions relatives à l'accès légal. En 2002, l'ABC a répondu à la consultation publique initiale du gouvernement fédéral au sujet de l'accès légal. En 2005, nous avons répondu à un document de consultation plus détaillé. En 2006, nous avons écrit aux ministres fédéraux de la Sécurité publique et de la Justice pour leur faire part de notre préoccupation relative au fait que les fournisseurs de services Internet répondaient aux demandes des organismes d'application de la loi sans autorisation législative précise. Ces réponses se poursuivent sous l'égide de la LPRPDE et d'autres lois : on a récemment annoncé qu'entre avril 2012 et mars 2013, l'Agence des services frontaliers du Canada avait demandé des renseignements sur des abonnés à l'Internet à 18 849 reprises. Quatre-vingt-dix-neuf pour cent de ces demandes ne reposaient pas sur une autorisation judiciaire, et les sociétés ont procuré l'information dans tous les cas sauf 25[11]. Plus récemment, nous étions prêts à répondre à plusieurs versions de projets de loi sur l'accès légal[12], lesquels sont morts au feuilleton ou ont été retirés par le Parlement.

La question de l'obtention sans mandat de l'identification d'abonnés a été prise en délibéré par la Cour suprême du Canada dans *R. c. Spencer*[13]. Avec les modifications que l'ABC propose dans le présent mémoire, nous estimons que les autres dispositions sur l'accès légal constituent une tentative viable d'adapter à la technologie actuelle les dispositions sur la perquisition, la fouille et la saisie du *Code criminel*. Les données et les communications par Internet font régulièrement partie de la preuve produite dans les affaires criminelles graves, allant du meurtre à la fraude de placement, de même que dans les poursuites proposées sur la cyberintimidation. Toutefois, les Canadiens ont des raisons d'être préoccupés car ils sont incapables de déterminer les renseignements que les organismes d'application de la loi ont à leur sujet, la façon dont ils ont été obtenus ou les fins auxquelles ils pourraient être utilisés.

Il faut s'occuper de cette situation, mais le *Code criminel* ne traite pas, et ne devrait pas traiter, des préoccupations générales en matière de vie privée. Le *Code* prévoit plutôt les enquêtes et

---

11 Paul McLeod, « Ottawa has been spying on you » (Chronicle Herald, 29 mars 2014).

12 Par exemple, le projet de loi C-51, *loi sur les pouvoir d'enquête au 21e siècle*.

13 2011 SKCA 144, dossier de la Cour suprême du Canada 34644.

les poursuites relatives aux infractions, y compris la saisie et l'admissibilité des données dans les affaires criminelles. Dans ce contexte, l'accusé a qualité pour soutenir que les données saisies contrairement à l'article 8 du la *Charte* doivent être écartées de la preuve. Toutefois, les instances criminelles ne touchent pas le droit à la vie privée des gens dont les renseignements sont obtenus par les organismes d'application de la loi lors d'enquêtes qui ne débouchent pas sur des accusations criminelles ni ne touchent le droit à la vie privée des gens dont les renseignements sont obtenus par les policiers car ils ont eu des contacts accessoires et innocents avec une personne susceptible d'être inculpée d'une infraction.

La conservation et l'utilisation de renseignements personnels de la part des organismes d'application de la loi sont régies par les diverses lois fédérales et provinciales sur la protection de la vie privée et le sort des documents. La conservation pendant une longue période de renseignements d'enquête est fondamentale pour le règlement des affaires non résolues (généralement des affaires d'homicides et d'agressions sexuelles) et pour les enquêtes sur des infractions continues en matière d'organisations criminelles. La divulgation de renseignements de la police met en danger ces enquêtes. La conservation pendant une longue période de renseignements d'enquête est aussi fondamentale pour l'issue des allégations d'erreur judiciaire.

Le gouvernement s'inquiète avec raison de l'efficacité des enquêtes criminelles en cette ère de données électroniques, mais un pouvoir accru de l'État de s'ingérer dans la vie privée doit s'accompagner de mécanismes de surveillance efficaces. Le fait cumulatif des diverses lois et mesures étatiques sur la vie privée doit être surveillé en vue de la préservation de l'équilibre entre l'application efficace de la loi et les droits de la personne.

RECOMMANDATION :

8. **L'Association du Barreau canadien recommande la création d'une entité unique chargée d'examiner l'effet, à l'échelle nationale, de la saisie, de la conservation et de l'utilisation de renseignements personnels par les organismes canadiens d'application de la loi.**

B. Les ordres et ordonnances de préservation

L'ordre de préservation des données informatiques (article 487.012)

Le projet d'article 487.012 prévoit qu'un agent de la paix ou un fonctionnaire public (agent) peut, sans autorisation judiciaire préalable, donner un ordre de préservation. Cet ordre oblige la personne visée à préserver les données informatiques en sa possession ou à sa disposition pour une période pouvant aller jusqu'à 21 jours.

L'agent aurait le pouvoir de donner un ordre de préservation s'il avait des motifs raisonnables de soupçonner, à la fois :

- qu'une infraction à une loi fédérale ou à « la loi d'un État étranger », dans ce dernier cas si une personne ou un organisme de l'État étranger enquête sur l'infraction, a été ou sera commise;
- que les données seront utiles à l'enquête.

L'ordre expirerait après 21 jours dans le cas d'une infraction soupçonnée à une loi fédérale ou après 90 jours dans le cas d'une enquête sur une infraction à la loi d'un État étranger, sauf si l'agent annulait l'ordre plus tôt. L'agent ne pourrait donner un autre ordre de préservation visant les mêmes données[14].

En outre, le projet d'article 487.0194 prévoit que dans les meilleurs délais après l'expiration de l'ordre ou son annulation, la personne dont les donnée sont en sa possession ou à sa disposition doit détruire les données qui ne seraient pas conservées dans le cadre normal de son activité commerciale sauf si les données « préservées » sont assujetties à une ordonnance subséquente en vertu de l'un des articles 487.13 à 487.17 (voir ci-après). Les données « préservées » devraient également être détruites après qu'un document les comportant est saisi en exécution d'un mandat (paragraphe 487.0194(4)).

L'article 487.012 (ordre de préservation des données informatiques) semble viser la préservation des données sans leur examen. Le pouvoir d'ordonner la préservation est tempéré par une disposition prévoyant qu'une fois l'ordre expiré, les données doivent être détruites si elles ne seraient pas conservées dans le cadre normal de son activité commerciale.

14 Projet de paragraphe 487.012(6).

Comme nous le soulignons dans l'analyse de plusieurs des dispositions suivantes du projet de loi, le seuil proposé des « motifs raisonnables de soupçonner » existe déjà dans la version actuelle de l'article 492.013 (ordonnance de communication de renseignements identifiant des titulaires de compte) et dans la version actuelle de l'article 492.1 (mandat de localisation). La Cour suprême du Canada a examiné le seuil du « soupçon raisonnable » pour d'autres types d'enquête[15].

Il peut y avoir des cas où il est impossible d'obtenir l'autorisation judiciaire suffisamment tôt pour préserver les données informatiques, mais cela est exceptionnel. À notre avis, s'il est impossible pour un agent d'obtenir une autorisation judiciaire préalable, l'ordre sans mandat de préserver les données devrait être en vigueur seulement pendant la période suffisante pour donner à l'agent la possibilité raisonnable de solliciter l'autorisation judiciaire – période beaucoup plus courte que les 21 jours proposés par le paragraphe 487.012(4).

RECOMMANDATION :

9. **L'Association du Barreau canadien recommande que les agents aient le pouvoir de donner un ordre de préservation seulement dans les cas d'urgence où ils ont des raisons de croire que les données en question pourraient être perdues ou détruites avant qu'une autorisation judiciaire ne puisse être obtenue. Dans ces cas exceptionnels, l'ordre de préservation devrait s'appliquer seulement pour la période raisonnablement nécessaire pour solliciter l'autorisation judiciaire.**

L'article 487.012 est rédigé de manière à permettre l'ordre de préservation s'il y a un soupçon raisonnable d'infraction à une loi fédérale ou d'infraction « à la loi d'un État étranger ». Cela permettrait l'ordre de préservation pour toute infraction à la loi étrangère, qu'elle soit de nature criminelle ou réglementaire, sans qu'il soit tenu compte de la gravité de l'infraction ou de la question de savoir si l'activité serait criminelle au Canada.

La collaboration entre pays pour l'application de la loi est importante, mais les ordres de préservation devraient être limités aux infractions criminelles prévues par les lois fédérales et aux infractions criminelles qui sont prévues par les lois d'États étrangers et qui constitueraient également des crimes au Canada.

15 *R. c. Chehil*, 2013 CSC 48; R. c. MacKenzie, 2013 CSC 50.

RECOMMANDATION :

10. L'Association du Barreau canadien recommande que si les agents se font octroyer le pouvoir de donner un ordre de préservation, ce pouvoir soit restreint aux cas où un agent a des motifs raisonnables de soupçonner la perpétration d'une infraction criminelle à une loi fédérale ou la perpétration d'une infraction criminelle à la loi d'un État étranger qui serait également un crime au Canada.

L'article 487.012 n'oblige pas l'agent à produire ou à tenir un registre des motifs à l'appui d'un ordre de préservation. La responsabilité, la transparence et la surveillance devraient toujours être inséparables des pouvoirs étatiques extraordinaires. Sans dossier écrit énonçant les motifs pour lesquels un agent a donné un ordre, il est impossible de maintenir ces mesures de protection fondamentales.

RECOMMANDATION :

11. L'Association du Barreau canadien recommande que si les agents se font octroyer le pouvoir de donner des ordres de préservation, des dossiers écrits devraient être exigés afin d'établir les motifs pour lesquels les ordres ont été donnés.

Le paragraphe (5) de l'article 487.012 conférerait aux agents le pouvoir d'assortir les ordres de préservation de conditions illimitées :

> (5) L'agent de la paix ou le fonctionnaire public qui donne l'ordre peut l'assortir des conditions qu'il estime indiquées, notamment pour interdire la divulgation de son existence ou de tout ou partie de son contenu. Il peut, par avis, annuler toute condition à tout moment.

À notre avis, il est inapproprié et injustifié d'accorder aux agents un pouvoir discrétionnaire absolu, particulièrement lorsque le manquement aux conditions imposées constitue une infraction criminelle. Les conditions pourraient empêcher une partie d'exercer les droits que lui confère la loi, sans mécanisme de contrôle judiciaire ou de surveillance. Si un « bâillon » est

justifiable dans certains cas, il devrait être imposé par un tribunal compétent, et non pas par un agent jouissant d'un pouvoir absolu.

RECOMMANDATION :

12. L'Association du Barreau canadien recommande l'omission du paragraphe 487.012(5) du projet de loi C-13.

L'ordonnance de préservation des données informatiques (article 487.013)

Le projet d'article 487.013 prévoit qu'un juge de paix ou un juge peut, sur demande *ex parte* d'un agent, rendre une ordonnance de préservation – ordonnance qui oblige la personne à préserver les données informatiques en sa possession ou à sa disposition pour une période pouvant aller jusqu'à 90 jours. Le juge aurait le pouvoir de rendre une ordonnance de préservation s'il estimait :

- qu'il y a des motifs raisonnables de soupçonner qu'une infraction à une loi fédérale ou à la loi d'un État étranger, dans ce dernier cas si une personne ou un organisme de l'État étranger enquête sur l'infraction, a été ou sera commise;
- qu'il y a des motifs raisonnables de soupçonner que les données sont en possession ou à la disposition de la personne;
- qu'il y a des motifs raisonnables de soupçonner que les données seront utiles à l'enquête relative à l'infraction;
- que l'agent a l'intention de demander, ou a demandé, la délivrance d'un mandat ou d'une ordonnance en vue d'obtenir un document comportant les données informatiques (le projet de loi définit le mot « document » comme « tout support sur lequel sont enregistrées ou inscrites des données »).

L'ordonnance de préservation proposée expirerait 90 jours après avoir été rendue, tant pour les enquêtes canadiennes qu'étrangères, sauf révocation antérieure. Dès que possible après l'expiration ou la révocation d'une ordonnance de préservation, la personne dont les données sont en sa possession ou à sa disposition devrait détruire les données qui ne seraient pas conservées dans le cadre normal de l'activité commerciale sauf si les données faisaient l'objet d'une nouvelle ordonnance de préservation ou d'une ordonnance de communication en vertu de l'un des articles 487.14 à 487.17 (voir plus loin). Les données « préservées » devraient

également être détruites après qu'un document les comportant est saisi en exécution d'un mandat (paragraphe 487.0194(4)).

Cette disposition semble viser la préservation des données sans examen de ces données. L'ordonnance de préservation est pondérée par la disposition prévoyant qu'une fois l'ordonnance expirée, les données doivent être détruites si elles ne seraient pas conservées dans le cadre normal de l'activité commerciale – toutefois, il semble que les mêmes données puissent faire l'objet d'ordonnances judiciaires de préservation consécutives.

Là aussi, le seuil des « motifs raisonnables de soupçonner » existe et a été examiné par la Cour suprême du Canada pour d'autres types d'enquête.

L'article 487.012 est rédigé de façon à permettre l'ordonnance de préservation en cas de soupçon raisonnable d'infraction à une loi fédérale ou de soupçon « qu'une infraction à la loi d'un État étranger a été commise ». Cela permettrait le prononcé d'une ordonnance de préservation pour toute infraction à une loi étrangère, de nature criminelle ou réglementaire, encore une fois sans qu'il soit tenu compte de la gravité de l'infraction ou de la question de savoir si l'activité serait criminelle au Canada.

L'ABC recommande que l'ordonnance de préservation prévue par l'article 487.012 soit limitée aux infractions criminelles aux lois fédérales et aux infractions criminelles aux lois d'États étrangers qui constitueraient également des crimes au Canada.

RECOMMANDATION :

13. **L'Association du Barreau canadien recommande que les ordonnances judiciaires de préservation soient limitées aux cas où le juge ou le juge de paix est convaincu qu'il y a des motifs raisonnables de soupçonner la perpétration d'une infraction criminelle à une loi fédérale ou la perpétration d'une infraction criminelle à la loi d'un État étranger qui constituerait également un crime au Canada.**

C. Les ordonnances de communication

L'ordonnance générale de communication de documents ou de données (article 487.014)

Il s'agit d'une révision renumérotée de l'article commun 487.012. La révision proposée clarifie l'ancien libellé, rehaussant vraisemblablement le seuil applicable aux ordonnances de communication. En vertu de la version actuelle de la disposition, le juge doit être convaincu qu'il y a des motifs raisonnables de croire qu'une infraction « a été ou est présumée avoir été commise »; en vertu du projet d'article 487.014, le juge doit être convaincu qu'il y a des motifs raisonnables de croire qu'une infraction « a été ou sera commise ».

L'ordonnance de communication en vue de retracer une communication donnée (article 487.015)

Le nouvel article 487.015 prévoit qu'un juge de paix ou un juge peut, sur demande *ex parte* présentée par un agent afin d'identifier tout dispositif ayant servi à la transmission de la communication ou toute personne y ayant participé, ordonner à toute personne (probablement un fournisseur de services) d'établir et de communiquer un document comportant des données de transmission qui ont trait à l'identification de ce dispositif ou de cette personne. On ne peut recourir à la disposition pour identifier une personne faisant l'objet d'une enquête relativement à certaines infractions (paragraphe 487.015(5)).

Le juge aurait le pouvoir de rendre l'ordonnance s'il était convaincu qu'il existe des motifs raisonnables de soupçonner, à la fois :

- qu'une infraction à une loi fédérale a été ou sera commise;
- que l'identification de tout dispositif ayant servi à la transmission d'une communication ou de toute personne y ayant participé sera utile à l'enquête relative à l'infraction;
- que les données de transmission en la possession ou à la disposition d'une ou de plusieurs personnes dont l'identité n'est pas connue permettront cette identification.

L'agent devrait transmettre un rapport écrit au juge qui a rendu l'ordonnance de communication dans les meilleurs délais après l'identification de l'auteur de la communication (paragraphe 487.015(6)). La personne visée par l'ordonnance de communication prévue à

l'article 487.015 en vue de retracer une communication à l'égard de données antérieurement préservées en vertu d'un ordre de préservation (article 487.012) ou d'une ordonnance de préservation (article 487.013) devrait détruire les données qui ne seraient pas conservées dans le cadre ordinaire de l'activité commerciale dans les meilleurs délais après la communication effectuée en vertu de l'ordonnance visée par l'article 487.015 ou dans les meilleurs délais après la révocation de l'ordonnance.

Cette disposition semble porter sur l'identification des « hôtes innocents » comme les réseaux WiFi publics. Nous le répétons, le seuil des « motifs raisonnables de soupçonner » figure déjà dans la version actuelle des articles 487.013 et 492.1 et a été examiné par la Cour suprême du Canada pour d'autres types d'enquête.

L'ordonnance de communication de données de transmission (article 487.016)

Le nouvel article 487.016 prévoit qu'un juge de paix ou un juge peut, sur demande *ex parte* présentée par un agent, ordonner à un tiers (un fournisseur de services) de communiquer un document comportant des données de transmission. Le juge aurait le pouvoir de rendre une telle ordonnance s'il était convaincu qu'il y a des motifs raisonnables de soupçonner, à la fois :

- qu'une infraction à une loi fédérale a été ou sera commise;
- que les données de transmission sont en la possession de la personne ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

La personne assujettie à une ordonnance de communication visée par l'article 487.016 relativement à des données antérieurement préservées en vertu d'un ordre de préservation (article 487.012) ou d'une ordonnance de préservation (article 487.013) devrait détruire les données qui ne seraient pas conservées dans le cadre ordinaire de l'activité commerciale dans les meilleurs délais après la communication effectuée en vertu de l'ordonnance visée par l'article 487.016 ou dans les meilleurs délais après la révocation de l'ordonnance. La norme des « motifs raisonnables de soupçonner » figure déjà aux articles 487.013 et 492.1. Toutefois, comme nous l'expliquons à la section D plus loin, les « données de transmission » peuvent révéler des « renseignements biographiques d'ordre personnel » à l'abri d'une perquisition, d'une fouille et d'une saisie en vertu de l'article 8 de la *Charte*, de sorte que le seuil plus élevé des « motifs raisonnables de croire » devrait être appliqué dans le projet d'article 487.016.

RECOMMANDATION :

14. L'Association du Barreau canadien recommande que, puisque les « données de transmission » peuvent révéler des renseignements biographiques d'ordre personnel à l'abri d'une perquisition, d'une fouille et d'une saisie en vertu de l'article 8 de la Charte, le seuil des « motifs raisonnables de croire » s'applique dans le projet d'article 487.016.

L'ordonnance de communication de données de localisation (article 487.017)

Le nouvel article 487.017 prévoit qu'un juge de paix ou un juge peut, sur demande *ex parte* présentée par un agent, ordonner à un tiers de communiquer un document comportant des données de localisation (p. ex., les données GPS en possession d'une société de location d'automobile). Le juge aurait le pouvoir de rendre une telle ordonnance s'il était convaincu qu'il y a des motifs raisonnables de soupçonner, à la fois :

- qu'une infraction à une loi fédérale a été ou sera commise;
- que les données de localisation sont en la possession de la personne ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

La personne assujettie à une ordonnance de communication visée par l'article 487.017 à l'égard de données de localisation antérieurement préservées en vertu d'un ordre de préservation (article 487.012) ou d'une ordonnance de préservation (article 487.013) devrait détruire les données qui ne seraient pas conservées dans le cadre normal de l'activité commerciale dans les meilleurs délais après la production effectuée en vertu de l'ordonnance visée par l'article 487.017 ou dans les meilleurs délais après la révocation de l'ordonnance. Le seuil des « motifs raisonnables de soupçonner » est utilisé et, nous le répétons, il existe déjà dans la version actuelle des articles 487.013 et 492.1 et a été examiné par la Cour suprême du Canada pour d'autres types d'enquête.

L'ordonnance de communication de « données financières » (article 487.018)

Il s'agit d'une révision renumérotée de l'ordonnance visée par la version actuelle de l'article 487.013 obligeant une institution financière à communiquer des renseignements identifiant un titulaire de compte. Comme la disposition existante, la version modifiée prévoit la communication des noms, adresses et dates de naissance des titulaires de comptes ainsi que

du type de compte, des numéros de compte, de l'état des comptes et des dates auxquelles les comptes ont été ouverts ou fermés. Cette disposition ne prévoit pas la communication de données relatives aux opérations financières.

Le juge aurait le pouvoir de rendre une telle ordonnance s'il était convaincu qu'il y a des motifs raisonnables de soupçonner, à la fois :

- qu'une infraction à une loi fédérale a été ou sera commise;
- que les données sont en la possession de l'institution financière ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

Le projet d'article 487.018 est essentiellement le même que la version actuelle de l'article 487.013, permettant aux juges d'ordonner aux institutions financières de communiquer des renseignements identifiant les titulaires de compte et les comptes. Une fois lesdits renseignements obtenus, un agent peut demander à un juge qu'il rende une ordonnance de communication générale, conformément à l'article 487.014, afin d'obtenir les renseignements concernant les opérations financières réalisées sur le ou les comptes indiqués.

Malheureusement, le titre de l'article 487.018, à savoir « Ordonnance de communication : données financières », fait naître la crainte que des données relatives à des opérations financières puissent être communiquées sans que soit atteint le seuil applicable à une ordonnance générale de communication, à savoir les motifs raisonnables de *croire* qu'une infraction « a été ou sera commise » (projet d'article 487.014). Le titre de l'article 487.018 devrait être modifié de manière à confirmer que l'article modifié a le même objet limité que la version actuelle de l'article 487.013.

RECOMMANDATION :

15. **L'Association du Barreau canadien recommande que le titre « Ordonnance de communication : données financières » soit modifié de manière à indiquer clairement que le nouvel article a le même objet limité que la version actuelle de l'article 487.013. Le titre recommandé est le suivant : « Ordonnance de communication de renseignements aux fins de l'identification des titulaires de comptes et des comptes ».**

D. Les mandats pour un dispositif de localisation et les mandats pour un enregistreur de données

Le mandat pour un dispositif de localisation (article 492.1)

Ce projet d'article révise la version actuelle de l'article 492.1, faisant passer le seuil applicable à la localisation des personnes physiques des « motifs raisonnables de soupçonner » aux « motifs raisonnables de croire ».

En vertu de la disposition modifiée, le juge peut délivrer un mandat pour un dispositif de localisation qui a trait à une « opération ou chose » s'il est convaincu qu'il y a des motifs raisonnables de *soupçonner*, à la fois :

- qu'une infraction à une loi fédérale a été ou sera commise;
- que la localisation du lieu d'une ou de plusieurs opérations ou du lieu ou des déplacements d'une chose, notamment un véhicule, sera utile à l'enquête relative à l'infraction.

Le juge pourrait délivrer un mandat pour un dispositif de localisation relatif à « une chose qui est habituellement portée ou transportée » par la personne s'il était convaincu qu'il y a des motifs raisonnables de *croire*, à la fois :

- qu'une infraction à une loi fédérale a été ou sera commise;
- que la localisation des déplacements d'une personne physique sera utile à l'enquête relative à l'infraction.

Le mandat pour un enregistreur de données de transmission (article 492.2)

Ce projet d'article remplace le mandat archaïque de l'art. 492.1 pour un enregistreur de numéros de téléphone par un nouveau mandat pour « un enregistreur de données de transmission ». En vertu de la nouvelle disposition, le juge pourrait délivrer un mandat autorisant un agent à obtenir des « données de transmission » au moyen d'un enregistreur de données de transmission s'il était convaincu qu'il y a des motifs raisonnables de *soupçonner*, à la fois :

- qu'une infraction à une loi fédérale a été ou sera commise;
- que les données de transmission seront utiles à l'enquête relative à l'infraction.

La définition de l'expression « données de transmission » et ses incidences

La documentation accompagnant le projet de loi C-13 indique que l'objet des dispositions proposées sur les données de transmission consiste à adapter les dispositions actuelles en matière de perquisition, de fouille et de saisie (combinées à la surveillance judiciaire) à l'ère numérique sans augmenter considérablement les pouvoirs de la police. Le sommaire du projet de loi énonce ce qui suit :

> Le texte modifie le *Code criminel* afin de prévoir notamment :
>
> > d) un mandat visant à élargir les pouvoirs d'enquête, actuellement restreints aux données relatives aux téléphones, aux données de transmission relatives à tout autre moyen de télécommunication.

L'ABC juge important que cette disposition ne permette pas la saisie de plus de renseignements que ce qui était permis en téléphonie prénumérique. Les données de transmission numériques diffèrent considérablement des données de signalisation prénumériques en téléphonie. Le projet de loi définit ainsi les « données de transmission » au nouvel article 487.011 et au nouveau paragraphe 492.2(6) :

> « données de transmission » Données qui, à la fois :
>
> a) concernent les fonctions de composition, de routage, d'adressage ou de signification en matière de télécommunication;
>
> b) soit sont transmises pour identifier, activer ou configurer un dispositif, notamment un programme d'ordinateur au sens du paragraphe 342.1(2), en vue d'établir ou de maintenir l'accès à un service de télécommunication afin de rendre possible une communication, soit sont produites durant la création, la transmission ou la réception d'une communication et indiquent, ou sont censées indiquer, le type, la direction, la date, l'heure, la durée, le volume, le point d'envoi, la destination ou le point d'arrivée de la communication;
>
> c) ne révèlent pas la substance, le sens ou l'objet de la communication.

En téléphonie prénumérique, les données de signalisation étaient le numéro originaire, le numéro destinataire, l'achèvement de l'appel et la durée de l'appel. Avec les communications numériques, les « données de transmission » et ce qu'elles révèlent sont différentes, notamment :

- l'adresse IP de l'ordinateur originaire;
- le programme d'ordinateur utilisé;
- le protocole de communication utilisé (p. ex. voix sur IP, vidéoconférence);
- l'adresse IP ou le nom de domaine du serveur ou de l'ordinateur avec lequel on communique;
- l'achèvement ou non de la transmission.

Même si le « contenu » est expressément exclu de la définition des données de transmission, ces données pourraient révéler des renseignements relatifs au contenu des communications. L'ABC craint que les données de transmission procurent aux organismes d'application de la loi des renseignements biographiques d'ordre personnel comme la fréquence des communications avec un fournisseur de soins de santé. Le droit à la vie privée à l'égard de telles communications entraîne l'application du droit de ne pas être soumis à une perquisition, à une fouille et à une saisie abusives en vertu de l'article 8 de la *Charte*.

RECOMMANDATION :

16. L'Association du Barreau canadien recommande que le paragraphe 492.2(1) soit modifié de manière à faire passer le seuil applicable aux mandats pour un enregistreur de données de transmission aux « motifs raisonnables de croire ».

E. Conclusion

La plupart des dispositions sur l'accès légal que renferme le projet de loi C-13 modifieraient les dispositions actuelles sur la perquisition, la fouille et la saisie du *Code criminel* (à l'exception des nouvelles dispositions relatives aux ordres et aux ordonnances de préservation). Toutefois, la technologie informatique a engendré un volume de données que n'auraient pas pu imaginer les rédacteurs des dispositions actuelles du *Code*, et la même technologie permet aux organismes d'application de la loi de saisir des quantités imprévues de données au moyen de leur reproduction électronique rapide.

Aucune disposition du *Code criminel* ne prévoit le retour ou la destruction des renseignements personnels copiés qu'obtiennent légalement les organismes policiers. Les articles 489.1 et 490 du *Code* prévoient un régime vénérable et lourd de retour des « choses » (pièces) saisies par la police, mais le paragraphe 490(13) permet déjà à la police de conserver indéfiniment des copies des documents saisis. Dans le projet de loi C-13, le paragraphe 487.0192(4) élargit cette approche, prévoyant que les articles 489.1 et 490 ne s'appliquent pas aux « documents » (tirés de données) qui sont saisis en vertu de l'une des dispositions modifiées sur les ordonnances de communication (articles 487.014 à 487.018).

Même si toutes les données saisies consistent en des « copies » de codes originaux, le contenu informationnel se retrouve en possession de la police. Hormis les données saisies en vertu d'ordonnances de communication, les données saisies en vertu de mandats pour un dispositif de localisation et pour un enregistreur de données de transmission pourraient également être qualifiées de « copies » susceptibles de conservation indéfinie.

Il existe de solides justifications à l'appui de la conservation de longue durée de renseignements d'enquête, mais compte tenu de la portée limitée du *Code criminel*, les modifications au *Code* proposées dans le projet de loi C-13 ne protègent pas suffisamment le droit à la vie privée dans le contexte des enquêtes électroniques. L'ABC demande instamment que cette question soit examinée hors du cadre de la procédure criminelle qu'établissent le *Code* et le projet de loi C-13.

RECOMMANDATION :

17. L'Association du Barreau canadien recommande au gouvernement fédéral d'effectuer un examen global indépendant du droit à la vie privée dans le contexte des enquêtes électroniques afin d'aller au-delà de l'application automatique de la procédure criminelle établie par le *Code criminel* et le projet de loi C-13.

IV. LES MODIFICATIONS À LA *LOI SUR LA CONCURRENCE*

L'ABC est préoccupée par les modifications proposées à la *Loi sur la concurrence* dans le projet de loi C-13 et estime que ces modifications devraient faire l'objet de consultations auprès des intéressés. En particulier, le projet de loi :

- permettrait au commissaire de la concurrence d'utiliser les ordonnances de préservation et de communication prévues par le *Code criminel* aux fins de ses enquêtes menées en vertu des dispositions d'examen de la *Loi sur la concurrence*;
- modifierait la définition de télémarketing de manière à élargir la portée du processus d'enquête du commissaire de la concurrence.

La plus importante de ces modifications proposées est l'application des outils d'enquête criminelle aux affaires non criminelles. L'ABC comprend qu'à l'égard de la partie VIII de la *Loi sur la concurrence*, le législateur a l'intention d'établir une distinction entre le comportement qui mérite une sanction criminelle et le comportement qui, bien que susceptible d'examen par le Tribunal de la concurrence, serait par ailleurs légal. Permettre le recours aux pouvoirs d'enquête criminelle dans le cadre des enquêtes menées en vertu de la partie VIII de la Loi mine cette distinction.

Les modifications à la *Loi sur la concurrence* proposées dans le projet de loi C-13 ont d'importantes incidences pour l'application de la Loi et devraient être mises en œuvre seulement après des explications supplémentaires et l'exposé des raisons pour lesquelles ces modifications sont nécessaires.

RECOMMANDATION :

18. **L'Association du Barreau canadien recommande que la *Loi sur la concurrence* ne soit pas modifiée de manière à permettre le recours à des ordres et ordonnances de préservation visant des tiers en vertu du *Code criminel* pour les enquêtes menées aux termes des dispositions non pénales de cette loi sur les pratiques susceptibles d'examen.**

19. **L'Association du Barreau canadien recommande que les modifications proposées à la Loi sur la concurrence, comme celles que prévoit le projet de loi C-13, qui risquent d'avoir des incidences en matière de politique sur la concurrence et d'application de la loi soient précédées de consultations auprès des intéressés.**

V. CONCLUSION

L'ABC apprécie l'occasion de formuler des commentaires sur le projet de loi C-13 et de faire part de ses suggestions en vue d'améliorer le projet de loi.