RESUME DES MEMOIRES PRESENTES DANS LE CADRE DE LA CONSULTATION SUR L'ACCES LEGAL

Nevis Consulting Group Inc.
Directeur de la rédaction

Le 28 avril 2003

TABLE DES MATIERES

CHAPITRE 1: INTRODUCTION

A. CONTEXTE

L'interception de communications et les perquisitions et les saisies de renseignements se sont avérées être des outils d'application de la loi efficaces pour la police et les organismes de sécurité nationale partout dans les pays développés. La même chose vaut pour le Canada où ces activités sont principalement menées par les forces policières et le SCRS[1] en vertu du *Code criminel* et la *Loi sur le Service canadien du renseignement de sécurité*. Dans plus de 90 % des cas où il y a eu dépôt d'une preuve obtenue par interception légale devant un tribunal en 2000, l'accusé a été déclaré coupable[2].

L'interception légale était jadis une pratique relativement simple lorsque la plupart des télécommunications mondiales étaient des conversations téléphoniques acheminées par des réseaux de circuits par câbles exploités par un petit nombre de grandes sociétés de téléphone. Une bonne partie de la législation canadienne en matière d'accès légal[3] a été adoptée durant cette période. Cependant, avec la déréglementation de l'industrie des télécommunications, l'Internet, les téléphones cellulaires, le courrier électronique sans fil, les réseaux de fibre optique à haute vitesse et le système vocal sur Internet (Voix sur IP[4]), les choses ont considérablement changé. Les organismes d'application de la loi[5] constatent que ces services plus avancés présentent des défis techniques et juridiques par rapport aux méthodes d'accès légal conventionnelles et que les dispositions législatives existantes ne permettent pas d'assurer une capacité d'interception efficace sur l'ensemble du réseau. Pendant ce temps, les éléments criminels emploient des équipements de communications qui ne peuvent pas être aisément interceptés par les organismes canadiens chargés de faire appliquer la loi et de protéger la sécurité nationale, même si ceux-ci ont légalement l'autorité voulue de le faire.

Le Canada doit aussi moderniser sa législation en matière d'accès légal s'il veut respecter ses obligations internationales dans la lutte contre le crime à l'échelle mondiale. Le Canada a signé la *Convention sur la cybercriminalité* du Conseil de l'Europe qui a pour objet de conférer aux États signataires les outils légaux nécessaires pour mener les enquêtes et les poursuites en matière de criminalité informatique, notamment les crimes commis en utilisant l'Internet et les crimes ayant trait à des documents électroniques. La *Convention* préconise aussi une plus grande coopération internationale dans la lutte contre la cybercriminalité et une harmonisation de la législation de chaque pays afin d'y parvenir. Avant que le Canada ne puisse ratifier la *Convention,* il faudra modifier le *Code criminel* pour inclure des dispositions sur les ordonnances de production, les ordonnances de conservation et la création d'une infraction relative aux virus informatiques ou autres dispositifs.

Dans le cadre du processus visant à mettre à jour la législation canadienne en matière d'accès légal, le ministère de la Justice du Canada, le Portefeuille du Solliciteur général du Canada[6] et Industrie Canada ont examiné différents moyens pour régler les problèmes liés à l'accès légal dans le cadre des technologies modernes des télécommunications. Un processus formel de consultation a ensuite été mis en branle auprès de représentants de l'industrie, de groupes de la société civile[7], d'organismes d'application de la loi, des commissaires à la protection de la vie privée et à l'information ainsi que le grand public afin de chercher à connaître leurs opinions sur les questions en jeu.

---

[1] Service canadien du renseignement de sécurité

[2] Rapport annuel du Solliciteur général sur la surveillance électronique, 2000 – www.sgc.gc.ca/policing/publications_f.asp

[3] L'interception par des organismes d'application de la loi ou de sécurité nationale et les perquisitions et les saisies par des organismes d'application de la loi.

[4] Voice over Internet Protocol.

[5] Dans le présent texte, les références aux « organismes d'application de la loi » s'entendent également des organismes de sécurité nationale, sauf si le contexte indique clairement le contraire.

[6] Le portefeuille du Solliciteur général désigne le ministère du Solliciteur général, la Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité (SCRS).

[7] Aux fins du présent rapport, les groupes de la société civile comprennent les groupes de défense des libertés fondamentales, les groupes communautaires, des représentants des consommateurs et des ONG s'intéressant aux questions de la protection des renseignements personnels et de l'accès à l'information et des associations du milieu juridique. Les commissaires à la protection de la vie privée et à l'information nommés par le gouvernement (et autres organisations similaires) qui ont participé à l'étude font l'objet d'une rubrique distincte à l'annexe C.

Un document intitulé *Accès légal - Document de consultation* a été publié en août 2002 pour servir de base à la discussion et encourager les divers intervenants à faire connaître leurs suggestions sur la meilleure façon de moderniser le cadre législatif canadien en la matière. On peut consulter ce document en ligne sur le site Internet du ministère de la Justice à l'adresse : www.Canada.justice.gc.ca/fr/cons/la_al .

> « Les objectifs de politique générale de ce processus sont de maintenir une capacité adéquate d'accès légal pour les organismes canadiens d'application de la loi et de sécurité nationale dans le contexte des nouvelles technologies et de préserver et protéger la vie privée et les autres droits et libertés des Canadiens et Canadiennes ».
>
> *Accès légal - Document de consultation*[8]

B. NATURE DU PRESENT RAPPORT

Le présent rapport fournit un résumé des mémoires présentés par des organismes d'application de la loi, des sociétés, des organisations et le grand public en réponse aux propositions contenues dans le document de consultation. La teneur des réponses a été substantielle et étendue. Les répondants ont fait de nombreuses suggestions utiles sur la façon dont les propositions contenues dans le document de consultation pourraient être améliorées, élargies, ou alors abandonnées. Certaines réponses exprimaient un souci sincère, quelques-unes ont permis la formulation d'arguments juridiques détaillés, alors que d'autres étaient remarquables pour leurs commentaires solides et francs.

Presque tous les mémoires contenaient des remarques qui mériteraient de se retrouver dans notre rapport. Malheureusement, il n'est possible d'inclure qu'un échantillon représentatif de ce que les gens ont dit. Cette tâche a été rendue plus facile, cependant, par la cohérence des opinions exprimées par les personnes interrogées dans chaque groupe sur un bon nombre de questions-clés.

Le rapport consiste en une introduction qui décrit le but poursuivi par la consultation sur l'accès légal et décrit le processus de consultation. Un aperçu général des réponses obtenues permet d'avoir un rapide portrait des opinions formulées. Il s'agit des dix commentaires les plus fréquemment exprimés par les personnes interrogées provenant de chaque groupe de participants : organismes d'application de la loi, industrie, commissaires à la protection de la vie privée et à l'information, groupes de la société civile et grand public.

Cette partie est suivie d'un compte-rendu détaillé des commentaires reçus de chacun des groupes et présentés essentiellement selon les mêmes rubriques que celles du document de consultation. Lorsqu'un groupe n'avait aucun commentaire à formuler sur ce sujet, aucune mention de la rubrique n'apparaît.

C. LE PROCESSUS DE CONSULTATION

Comme nous l'avons mentionné plus haut, des Canadiens ont été invités à se pencher sur des questions relatives à l'accès légal et des options de changement, fondées sur le document de consultation. La période de consultation a débuté au mois d'août 2002 et le délai pour faire connaître ses commentaires a été fixé au 15 novembre 2002. Cette échéance a par la suite été prolongée au 16 décembre 2002 en réponse à des demandes écrites de la part de plusieurs des parties intéressées.

De plus, le processus de consultation a donné lieu à plus de 20 réunions entre les principaux intervenants et des représentants des ministères gouvernementaux visés[9]. Ces rencontres ont permis aux participants d'une part, de mieux comprendre les objectifs du gouvernement avant la préparation de leurs réponses formelles et d'autre part de demander des précisions sur des questions les intéressant plus particulièrement. Parmi les participants, on pouvait compter des représentants d'organismes d'application de la loi, d'associations ou de sociétés du secteur privé, d'organisations de défense des droits fondamentaux et de protection de la vie privée, de gouvernements provinciaux

[8] Page 6.
[9] Le ministère de la Justice, le Portefeuille du Solliciteur général et Industrie Canada.

ainsi que le Commissaire à la protection de la vie privée du Canada. Le grand public a été invité à répondre au document de consultation par la poste et par courrier électronique.

D. LA REPONSE DES CANADIENS

La contribution des organismes d'application de la loi a essentiellement pris la forme d'un document exhaustif présenté par l'Association canadienne des chefs de police (ACCP), appuyé par des exposés écrits provenant de 55 services de police, y compris de nombreux détachements de la GRC d'un peu partout au Canada. Quelques services de police ont formulé des commentaires additionnels basés sur leur expérience régionale.

Le secteur de l'industrie a contribué au processus avec 19 réponses provenant de sociétés œuvrant dans le domaine des télécommunications et d'associations d'industries connexes, alors que cinq commissaires à la protection de la vie privée et à l'information au Canada ont fourni leurs points de vue.

Au total, 14 groupes de la société civile ont présenté des mémoires portant surtout sur des questions relatives au respect du droit à la vie privée et des droits de la personne. Deux de ces organisations ont leur siège social aux États-Unis et ont pu faire part de leur expérience avec une législation semblable adoptée par le Congrès au cours des dernières années.

Des réponses ont été reçues de 219 individus - presque tous des Canadiens[10]. La plupart ont été acheminées par courrier électronique. Certaines exprimaient une opposition catégorique aux propositions formulées, alors que d'autres appuyaient fortement le processus de consultation. L'Ontario a fourni environ 50 % des réponses, la Colombie-Britannique et l'Alberta 38 %, et le Québec 7 %. Approximativement 2 % des réponses provenaient de femmes.

[10] Certaines réponses étaient anonymes ou ne comportaient pas d'indication du lieu d'où elles provenaient, et il est donc impossible d'être certain de leur contenu canadien.

CHAPITRE 2 : APERÇU GENERAL DES REPONSES

2.1 ORGANISMES D'APPLICATION DE LA LOI

1. Les services policiers ont fortement appuyé les propositions en général.

2. La capacité de la police d'accéder légalement aux services de télécommunications n'a pas suivi les progrès de la technologie en matière de communications. Cette lacune crée une zone sûre à l'intérieur de laquelle les auteurs de crimes graves peuvent communiquer sans crainte de détection. La police doit être techniquement en mesure d'intercepter tous les services de télécommunications offerts au Canada sans exception.

3. Les fournisseurs de services de communication (FSC)[11] devraient être tenus d'assumer le coût d'installation des dispositifs d'accès légal lorsque leurs installations sont nouvelles ou ont été sensiblement améliorées. Le gouvernement devrait leur interdire de recouvrer, directement ou indirectement, les coûts d'infrastructure auprès des organismes d'application de la loi, par exemple en les intégrant aux frais de service ou de connexion.

4. En principe, les FSC doivent pouvoir recouvrer les frais raisonnables engagés pour prêter main forte aux organismes d'application de la loi. Ces coûts doivent être répartis sur une grande échelle (comme les frais actuels du service 911) plutôt que perçus des différents services de police. Toutefois, il ne faut pas permettre aux FSC d'imposer des frais ou d'autres charges à titre de condition de conformité avec une ordonnance judiciaire.

5. Il y a lieu de mettre en place un mécanisme d'application indépendant du gouvernement afin d'assurer le respect de la loi.

6. L'exemption quant à la capacité d'interception doit être l'exception plutôt que la règle. Il y a lieu d'obliger les FSC à présenter un plan de mise en œuvre avec chaque demande d'exemption ainsi qu'un rapport trimestriel indiquant en détail les mesures qui seront prises pour que la loi soit respectée.

7. Il faut imposer de lourdes amendes aux FSC qui ne respectent pas les exigences obligatoires en matière de capacité d'interception. La collaboration étroite entre les fournisseurs de services et les organismes d'application de la loi permettra de surmonter la vaste majorité des difficultés. Seules les contraventions les plus graves et les plus flagrantes par rapport aux normes établies dans la législation proposée nécessiteraient une action de la part des forces de l'ordre.

8. L'interception légale par la police de communications privées au Canada doit continuer d'être assujettie à l'autorisation préalable du tribunal.

9. Les NAA et l'IFSL[12] ne constituent pas des renseignements personnels et les organismes d'application de la loi ne doivent pas avoir besoin d'une autorisation judiciaire pour y avoir accès. Il y a lieu de prévoir une disposition dans la loi obligeant les FSC à fournir ces renseignements aux organismes d'application de la loi et de sécurité nationale. Si cette suggestion est rejetée pour des motifs ayant trait au respect de la vie privée, il y aurait alors lieu d'envisager une ordonnance de production assujettie à des règles simplifiées.

10. Afin de lutter contre la criminalité croissante à l'échelle internationale, les pouvoirs relatifs à l'accès légal accordés au Canada aux organismes d'application de la loi doivent être harmonisés avec ceux qui sont disponibles dans d'autres pays. L'Australie, les Pays-Bas, la Nouvelle-Zélande le Royaume-Uni et les États-Unis ont pris une longueur d'avance sur le Canada en adoptant une législation en matière d'accès légal qui est conforme à la nouvelle technologie d'aujourd'hui.

[11] On trouvra à la page 20 les types de fournisseurs formant la catégorie de FSC dans le présent rapport.
[12] NAA – nom et adresse de l'abonné. IFSL - identité du fournisseur de services locaux.

2.2 INDUSTRIE

1. La plupart des FSC qui ont répondu appuyaient la nécessité de permettre un accès légal efficace compte tenu des changements technologiques[13].

2. Le document de consultation est trop vague et imprécis pour permettre autre chose que des commentaires très généraux. Avant le dépôt d'un projet de loi devant le Parlement, on devra tenir d'autres consultations, notamment afin d'obtenir des commentaires sur les propositions précises contenues dans l'avant-projet de loi et les règlements qui l'accompagneront.

3. L'interception du courrier électronique non ouvert et de communications numériques similaires en transit doit être considérée comme l'interception d'une « communication privée », et donc assujettie aux garanties offertes relativement à une autorisation sous le régime de la Partie VI du *Code criminel*. Pour avoir accès au courrier électronique qui a été ouvert et que l'usager a décidé de conserver, les organismes d'application de la loi devraient être tenus d'obtenir un mandat de perquisition ou une ordonnance de production.

4. Les circonstances justifiant une ordonnance d'exemption devraient être précisées, ainsi que les critères permettant de déterminer quand et pendant combien de temps ces ordonnances seront valides. Toute règle concernant le pouvoir d'exemption doit être claire et transparente.

5. La législation proposée doit veiller à ce que les organismes d'application de la loi assument les frais raisonnables engagés par les fournisseurs de services pour les aider à mener à bien leurs opérations d'interception légale, de saisie ou d'exécution d'une ordonnance de conservation. Ces frais devraient être négociés entre chaque fournisseur de services et l'organisme concerné, plutôt que d'êtres précisés à titre de tarifs universels dans les règlements. Industrie Canada et le Solliciteur général, ou encore un arbitre indépendant, devraient agir comme médiateur en cas de différend entre un FSC et un organisme d'application de la loi.

6. Les définitions fournies dans le document de consultation diffèrent de celles que l'on trouve dans la *Loi sur les télécommunications*. Certains termes importants comme « capacité de base d'interception » ne sont pas définis. Des définitions claires et cohérentes conformes à celles qui sont employées à l'échelle internationale sont essentielles au succès de la législation proposée.

7. Jusqu'à ce que des solutions techniques soient disponibles relativement à l'équipement de transmission utilisé par les fournisseurs de services, et que ces solutions puissent être mises en place et appliquées moyennant un coût additionnel minime pour le fournisseur de services, le gouvernement devrait assumer les coûts au titre de la « capacité de base d'interception », peu importe la définition donnée aux expressions « nouvelles technologies ou nouveaux services » et à « amélioration significative » dans la nouvelle loi.

8. Le document de consultation n'a pas démontré que les dispositions actuelles de la loi ne permettent pas un accès efficace aux services de communication de données au Canada ou que des enquêtes et des poursuites ont échoué en raison d'une absence de capacité technique.

9. Les fournisseurs de services s'opposent fortement à l'obligation de recueillir, stocker ou garantir l'exactitude des renseignements sur les abonnés au-delà de ce qui est nécessaire pour leurs propres besoins d'affaires.

10. Les fournisseurs de services sont aussi fortement opposés à la création de toute base de données nationale relative à leurs abonnés, invoquant des motifs liés à la protection de la vie privée et à la sécurité, ainsi que le coût élevé associé à la création et à la mise à jour d'une telle base de données. Ils font remarquer que la plupart des cybercriminels sont tout à fait capables d'utiliser de faux noms, des comptes piratés ou des terminaux d'accès publics pour leurs communications ou transactions.

[13] Les autres n'avaient pas de commentaire à formuler sur cette question.

2.3 COMMISSAIRES A LA PROTECTION DE LA VIE PRIVEE ET A L'INFORMATION

1. Le document de consultation ne démontre pas en quoi les mesures proposées sont nécessaires.

2. Les nouvelles technologies et les nouveaux services de communications présenteront sans doute des défis pour les organismes d'application de la loi et obligeront les FSC à leur fournir des capacités de base en matière d'interception et de surveillance afin qu'ils puissent avoir un accès légal.

3. Les mesures proposées vont bien au-delà de ce qui est nécessaire pour maintenir les capacités existantes face à la technologie moderne de communications.

4. Les courriels ne doivent pas être soumis à une norme de protection moins stricte que celle appliquée aux appels téléphoniques ou aux lettres. De même, le furetage sur Internet ne doit pas être moins bien protégé que l'achat de livres ou les recherches dans une bibliothèque de référence.

5. Les Canadiens ont le droit de croire que leurs communications et activités en ligne ne seront pas interceptées ou scrutées de près arbitrairement.

6. Si la *Convention sur la cybercriminalité* autorise une violation injustifiable du droit à la vie privée des Canadiens qui serait incompatible avec nos valeurs et nos droits, le gouvernement canadien doit refuser de la ratifier.

7. Le gouvernement doit continuer de résister à toute suggestion voulant que les exigences relatives au stockage des données générales fassent partie de l'initiative relative à l'accès légal.

8. Il n'y a pas lieu de créer une base nationale de données pour les NAA et l'IFSL. Il n'est nullement nécessaire de changer les lois et les pratiques actuelles en ce qui a trait à l'accès à ce type de renseignements.

9. L'obligation faite à ceux qui vendent des téléphones cellulaires ou des cartes d'appel prépayées de recueillir des renseignements confidentiels sur les acheteurs, comme leur numéro de permis de conduire ou de carte de crédit, constituerait une grossière ingérence dans leur vie privée.

10. Le document de consultation n'indique pas que l'on envisage des mécanismes de reddition de compte .

2.4 GROUPES DE LA SOCIETE CIVILE

1. Le document de consultation n'explique pas clairement les propositions du gouvernement du Canada.

2. L'avant-projet de loi et les règlements d'application doivent être diffusés pour que le public puisse les examiner exhaustivement et que les parties intéressées aient suffisamment de temps pour en évaluer l'impact et soumettre des commentaires.

3. Le document n'explique pas de manière convaincante comment les propositions contribueraient effectivement à lutter contre le crime organisé ou le terrorisme. Le gouvernement aura sans doute un accès plus grand à la vie privée des Canadiens, mais les criminels et les terroristes dangereux ne seront vraisemblablement pas imprudents au point de se voir assujettir aux mesures proposées.

4. Si des éléments d'information justifient les mesures proposées, il faut les rendre publics pour que l'on puisse vérifier si les avantages sur le plan de la sécurité l'emportent sur les inconvénients liés à une atteinte à la vie privée. En l'absence de tels éléments, les mesures doivent être abandonnées.

5. Les propositions établiraient une norme moins exigeante pour l'interception légale, les perquisitions et les saisies de communications en ligne que pour les communications téléphoniques ou postales, par exemple. Aucune justification n'a été donnée pour expliquer cette approche. Les normes prévues dans le *Code criminel* devraient être les mêmes quelle que soit la technologie utilisée.

6. Tout nouveau texte législatif doit contenir des dispositions spécifiques aux questions relatives au respect de la vie privée chaque fois qu'il y a un risque d'atteinte à la vie privée d'une personne. Des références d'ordre général à la *Charte canadienne des droits et libertés* (la *Charte*) et à la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDE*) sont insuffisantes.

7. Le gouvernement n'a pas démontré qu'une infrastructure de surveillance aussi massive était nécessaire. Ainsi, on ignore combien d'enquêtes ont été sérieusement affectées en raison d'une absence de capacité technique.

8. Si les organismes d'application de la loi éprouvent des difficultés avec les nouvelles technologies de communications, la solution n'est pas d'abaisser les normes juridiques en matière d'interception, mais plutôt de leur fournir l'expertise technique et l'équipement dont ils ont besoin pour fonctionner dans l'environnement en évolution.

9. Les propositions exigent des clients ou de leurs fournisseurs de services de communication qu'ils paient pour la surveillance. Cela est mauvais en principe et irréalisable dans les faits.

10. Les fournisseurs de service Internet (FSI) ont pour tâche de fournir des services à leurs clients. Cette tâche ne doit pas consister également à les surveiller au nom de l'État. On ne doit pas se servir d'ordonnances de production dans le but de se soustraire aux critères exigeants qu'il faudrait respecter si les organismes d'application de la loi procédaient eux-mêmes à la perquisition ou à l'interception.

2.5 GRAND PUBLIC

1. Le grand public est très reconnaissant d'avoir eu l'occasion de formuler des commentaires sur ces propositions.

2. On ne sait pas exactement quel avantage présente les modifications législatives proposées, que n'offre pas déjà la législation actuelle.

3. Il est fort inquiétant que des traités internationaux comme *la Convention sur la Cybercriminalité* soient signés sans consultation démocratique et présentés ensuite au public comme s'il était essentiel qu'ils soient ratifiés.

4. Le document de consultation ne réussit pas à démontrer comment l'Internet a créé « des problèmes importants pour les enquêteurs ». Aussi, dans le cas de l'Internet, « la nécessité de disposer d'équipement de pointe » semble se résumer à l'existence de renifleurs de paquets qui sont largement employés par les fournisseurs de service Internet et coûtent quelques milliers de dollars chacun.

5. On n'établit pas dans le document de consultation de justification à l'effet que les Canadiens méritent moins de protection de leur vie privée lorsqu'ils utilisent des technologies de communication numériques plutôt qu'analogiques, ou en fait lorsqu'ils utilisent des moyens électroniques plutôt qu'un moyen traditionnel.

6. Le cryptage des données est largement employé par les criminels et les terroristes lorsqu'ils communiquent sur des réseaux privés et publics, y compris l'Internet. Les techniques de cryptage sont souvent indétectables, impossibles à intercepter et elles peuvent rendre inefficaces les techniques d'interception utilisées par les organismes d'application de la loi et les fournisseurs de services de communication.

7. S'il a besoin de l'aide d'un fournisseur de services et que cela entraîne pour ce dernier des coûts supérieurs à ses coûts d'exploitation normaux, l'organisme d'application de la loi devrait assumer ces coûts. Ils ne devraient pas être assumés par le fournisseur de service ni refilés au client.

8. Aucun fournisseur de services de communication ne devrait agir comme organisme de collecte de renseignements pour le compte du gouvernement canadien. S'il veut obtenir de l'information, et en a besoin, le gouvernement devrait faire la recherche de données, les recueillir et les stocker. Le fournisseur de services de communication ne doit être tenu de fournir les installations que lorsqu'il existe une ordonnance légitime à cet effet.

9. Nous n'avons nullement besoin d'une autre base de données pancanadienne de dossiers personnels. Il n'y a pas de registre pancanadien d'usagers du téléphone ou de la poste, et il ne devrait pas y en avoir non plus pour les usagers de l'Internet. Une banque de données de cette nature constituerait une dangereuse accumulation de renseignements. Les bureaucrates peuvent-ils garantir que cette base de données ultra-sensibles ne sera jamais piratée ?

10. L'interception du courrier électronique devrait nécessiter une ordonnance judiciaire quel que soit le point d'interception.

CHAPITRE 3 : COMMENTAIRES FORMULES PAR LES ORGANISMES D'APPLICATION DE LA LOI

NOMBRE TOTAL DE MEMOIRES REÇUS : 58

L'Association canadienne des chefs de police a soumis une réponse au document de consultation sur l'accès légal au nom des organismes d'application de la loi canadiens[14]. La plupart des services de police ont de plus écrit des lettres distinctes indiquant leur appui au mémoire de l'ACCP. Quelques détachements de la GRC ont fait savoir qu'ils appuyaient l'initiative concernant l'accès légal. Plusieurs services de police avaient des observations additionnelles à formuler et elles ont été incluses dans le résumé. Étant donné le sujet traité, les mémoires présentés par deux ministères ont aussi été inclus dans ce chapitre. On trouvera à l'annexe A la liste des organismes d'application de la loi et à l'annexe E celle des ministères du gouvernement.

A. GENERALITES

1. Les technologies de communication ont continué d'évoluer rapidement, mais non la capacité de la police d'accéder aux services de télécommunications et de recueillir les renseignements nécessaires pour appréhender les criminels. Cette lacune permet aux criminels de communiquer entre eux sans crainte de détection ou d'arrestation.

2. Selon les organismes canadiens d'application de la loi, il existe quelques grands principes qui sont très importants dans cette discussion :

- Les cas d'interception de communications privées par la police canadienne doivent continuer de faire l'objet d'une autorisation judiciaire préalable.

- La capacité technique de procéder à une interception ordonnée par le tribunal doit toujours exister et ne pas être compromise. Il ne doit pas y avoir de « zones sûres »[15] où l'interception ne serait pas possible au Canada.

- Les nouvelles technologies de communications ne posent pas problème en elles-mêmes. Toutefois, si elles ne sont pas réglementées et en l'absence de contrepoids, elles peuvent avoir des conséquences négatives imprévues. Il faut des mécanismes juridiques modernes de façon à ce que nous, comme société, assurions un équilibre entre la nécessité de demeurer concurrentiel à l'échelle mondiale et celle de garantir la sécurité publique.

- Les technologies modernes de communications réduisent les distances et libèrent des contraintes géographiques, et les criminels organisés, les prédateurs sexuels sur Internet et les terroristes en profitent. La législation canadienne doit tenir compte de l'augmentation de la criminalité transfrontalière.

- Certains fournisseurs de services imposent des frais substantiels aux organismes d'application de la loi avant de procéder à une interception ordonnée par un tribunal. Personne, qu'il s'agisse d'une personne morale ou physique, ne peut miner l'autorité de la cour en imposant des frais ou autre obligation financière comme condition de conformité avec une ordonnance judiciaire légitime.

---

[14] Rédigé par le Comité de modifications aux lois de l'ACCP et le Sous-comité de surveillance électronique légalement autorisée (SELA). Celui-ci est un groupe permanent formé d'experts dans le domaine de l'accès légal provenant des services policiers fédéraux, provinciaux et municipaux et de services nationaux de sécurité. On trouvera le texte intégral de la réponse de l'ACCP (en anglais) à l'adresse: www.cacp.ca

[15] L'ACCP définit ces zones sûres comme étant toute technologie, application ou dispositif qui, utilisés comme moyens de communication, de par sa conception ou de par son utilisation avec d'autres technologies, applications ou dispositifs, ont pour effet d'empêcher ou de nuire, intentionnellement ou non, à l'identification ou l'interception de la communication.

3. L'Internet à haute vitesse et les services modernes de communication sans fil sont des outils utiles pour l'ensemble des Canadiens. En même temps, la police est de plus en plus aux prises avec des criminels subtils qui emploient ces mêmes technologies de télécommunications pour commettre des actes illégaux et entraver les efforts que la police déploie pour les traduire en justice.

4. Les pouvoirs qui existent au Canada en matière d'accès légal doivent être harmonisés avec ceux qui sont disponibles dans d'autres pays afin de lutter contre la criminalité internationale croissante. L'Australie, la Nouvelle-Zélande, la Grande-Bretagne, les Pays-Bas et les États-Unis ont une avance sur le Canada du fait qu'ils ont adopté des lois en matière d'accès légal en harmonie avec la technologie d'aujourd'hui.

5. Les dispositions touchant l'accès légal doivent être transparentes, ce qui signifie qu'elles devraient clairement établir la procédure applicable à suivre selon le type de données et l'attente connexe en matière de respect de la vie privée. Elles doivent aussi être transparentes en ce sens qu'elles sont formulées dans des termes aussi neutres que possible au plan technologique.

B. OBLIGATION DE GARANTIR LA CAPACITE D'INTERCEPTION

1. La norme minimale acceptable est que tous les services de télécommunications, nouveaux ou améliorés de façon significative, doivent permettre l'interception ; l'objectif est que tous les services de télécommunications au Canada soient dotés des dispositifs permettant l'interception à l'intérieur d'un délai précis stipulé par la loi.

2. Les FSC devraient être techniquement en mesure de fournir aux organismes d'application de la loi et de sécurité nationale un accès en temps réel à l'information ci-après, peu importe l'étendue des services offerts aux abonnés :

1. Les télécommunications de la personne faisant l'objet d'une ordonnance d'interception, à l'exclusion de toute autre télécommunication non visée par l'ordonnance; l'information interceptée doit être communiquée uniquement à l'organisme d'application de la loi ou de sécurité nationale précisé.

2. L'ensemble des télécommunications de la personne, y compris le contenu, ce qui permet à l'organisme autorisé de procéder à une surveillance en temps réel pendant toute la durée de l'interception.

3. Toutes les tentatives de la personne d'établir des télécommunications.

4. L'existence d'un mécanisme permettant de rattacher précisément les données relatives aux télécommunications[16] au contenu de l'appel.

5. Les mesures matérielles, personnelles et administratives utilisées pour garantir la sécurité relativement aux interceptions.

6. Les télécommunications cryptées par le FSC devant être livrées aux organismes autorisés *en clair*.

7. Les renseignements de localisation les plus précis dont dispose le réseau de FSC.

C. REGLEMENTS

1. Les règlements doivent non seulement respecter les normes internationales, mais être efficaces et opérationnels au Canada.

2. Des règlements seront nécessaires pour permettre aux organismes d'application de la loi d'avoir accès tant au contenu des communications qu'aux données relatives au trafic de manière à ce que les deux puissent être présentés en preuve devant les tribunaux.

[16] Synonyme de « données sur le trafic » ou « données relatives au trafic » dans le présent rapport.

3. Les fournisseurs de services de communication doivent permettre à la police d'examiner seulement les données ciblées dans une ordonnance précise du tribunal. Ils devraient aussi garantir la confidentialité et la sécurité du contenu de la communication interceptée, des données relatives au trafic et de l'identité des personnes en cause.

4. Les règlements devraient définir la capacité requise pour l'interception simultanée chez les fournisseurs de services, les exigences en matière de sécurité pour les opérations de police, ainsi que l'intégrité, la compétence et la fiabilité du personnel du fournisseur.

5. Les règlements devraient interdire aux FSC de recouvrer les coûts d'infrastructure auprès des organismes d'application de la loi et de sécurité nationale, par exemple en les intégrant aux frais de service ou de connexion.

D. EXEMPTION

1. L'exemption quant à la capacité d'interception doit être l'exception plutôt que la règle.

2. Les différends entre les organismes d'application de la loi et les fournisseurs de services de communication ainsi que les demandes d'exemption doivent être tranchés par un organisme indépendant relevant du Solliciteur général et du ministre de l'Industrie ou par un comité formé de trois personnes nommées par le Cabinet et représentant le Solliciteur général, Industrie Canada et le Sous-comité de la surveillance électronique légalement autorisée (SLEA) de l'ACCP.

3. Les dispositions relatives à l'exemption dans le projet de loi devraient devenir inopérantes et aucune nouvelle demande d'exemption ne devrait être acceptée cinq ans après que la loi a reçu la sanction royale.

4. Les demandes d'exemption devraient être traitées dans les 90 jours suivant leur réception et au cours de cette période, les demandeurs ne devraient pas encourir de peines financières ou autres prévues par la loi.

5. Une exemption ne doit pas être accordée pour les interceptions visées aux points 1, 2, 3, 4 et 6 (B2) dans les cas où elle aurait pour effet de créer « une zone sûre » où l'interception ne serait pas possible.

6. On doit exiger que les FSC soumettent avec chaque demande d'exemption un plan de mise en œuvre, assorti d'un compte-rendu trimestriel, expliquant en détail comment ils parviendront à se conformer pleinement à la législation. La durée maximale d'une exemption ne doit pas dépasser 12 mois. Au terme de cette période, le fournisseur de services de communication doit pleinement se conformer à la loi ou demander une prolongation de 12 mois, qui serait évaluée comme s'il s'agissait d'une nouvelle demande.

E. MECANISME DE CONFORMITE

1. Le projet de loi devrait prévoir un mécanisme de conformité dont l'application ne relève pas du gouvernement, qui est efficace et efficient et dispose des fonds et ressources nécessaires. Ce mécanisme devrait aussi servir à la prise de décisions relatives aux demandes d'exemption et comporter un appel auprès du Cabinet fédéral (D2).

2. Des amendes élevées devraient être imposées en cas de non-respect de l'obligation de garantir la capacité d'interception[17].

3. La collaboration étroite entre les fournisseurs de services et les organismes d'application de la loi permettra de surmonter la vaste majorité des difficultés. Seules les contraventions les plus graves et les plus flagrantes par rapport aux normes établies dans la législation proposée nécessiteraient une action de la part des forces de l'ordre.

[17] L'ACCP signale que les sociétés en Australie sont passibles d'amendes maximales de dix millions de dollars australiens en cas de manquements graves et flagrants à la loi.

F. COUTS

1. Les fournisseurs de services de communication devraient être tenus d'assumer en entier le coût d'installation des dispositifs d'accès lorsque leurs installations sont nouvelles ou ont été sensiblement améliorées.

2. Même lorsque la capacité d'intercepter existe et que les tribunaux ont autorisé l'interception, certains fournisseurs de services de communication ont tenté d'imposer des frais importants à la police ce qui a donné lieu à la conclusion de regrettables ententes spéciales entre des organismes d'application de la loi et des sociétés de télécommunications individuelles. Les organismes d'application de la loi maintiennent que ces coûts touchent l'intérêt public et exhortent le gouvernement à légiférer afin d'interdire catégoriquement aux FSC d'exiger des frais pour se conformer à une ordonnance du tribunal. Il faut aussi empêcher les fournisseurs de services de communication de récupérer les coûts de l'infrastructure des organismes d'application de la loi [18].

3. Certains FSC facturent des frais de consultation aux organismes d'application de la loi pour des renseignements sur leurs abonnés, tandis qu'ils fournissent gratuitement ces renseignements au public, comme l'accès à la base de données sur l'identité du fournisseur de services locaux (IFSL) sur la toile. Rien ne semble pouvoir justifier cette pratique. Tous les frais exigés pour des recherches plus poussées, comme un historique des télécommunications par sujet, devraient prendre en compte la facilité avec laquelle les fournisseurs de services peuvent avoir accès aux renseignements demandés grâce à leurs bases de données internes ou autres dispositifs modernes auxquels ils peuvent avoir accès rapidement.

4. Les lignes de retour aux fins du transfert du matériel intercepté du fournisseur de services de communication à la police ou au service de sécurité nationale sont facturées par les transporteurs canadiens aux taux commerciaux, conformément aux règlements du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC). L'élargissement de la bande passante requise pour les nouvelles technologies de communications fait grimper ces coûts. On doit accorder aux organismes d'application de la loi et de sécurité nationale des tarifs réduits conformément à l'article 27 de la *Loi sur les télécommunications*.

5. Les organismes d'application de la loi reconnaissent que les fournisseurs de services de communication doivent être en mesure de recouvrer les dépenses raisonnables engagées pour donner suite à une ordonnance du tribunal, mais s'opposent énergiquement à ce que ces frais soient payés par les services de police puisque la plupart d'entre eux n'en ont pas les moyens.

6. Le recouvrement des coûts par les fournisseurs de services de communication devrait être établi suivant une formule de répartition large et équitable, raisonnable et proportionnelle à l'aide effectivement fournie, un peu comme les frais du service 911. Les frais devraient aussi faire l'objet d'un contrôle par une tierce partie indépendante.

7. Tous les frais imposés par les fournisseurs de services de communication, autorisés par la législation proposée, doivent être uniformes et appliqués conformément à une pratique courante à l'échelle du Canada. Ils devraient faire l'objet d'un examen tous les deux ans et une date précise devrait être fixée pour l'entrée en vigueur des modifications.

8. À partir d'une date fixée par le Cabinet, les fournisseurs de services de communication devraient disposer d'un délai précis pour fournir des renseignements sur les capacités d'interception offertes par leur réseau. Les renseignements ainsi fournis au sujet des mises à niveau ou modifications requises pour respecter la loi devraient servir à déterminer le montant de l'aide ou du remboursement que recevra le fournisseur afin de satisfaire aux exigences.

G. ORDONNANCES GENERALES DE PRODUCTION

1. Les ordonnances de production du type décrit dans le document de consultation sont justifiées dans le monde d'aujourd'hui. Les tiers possesseurs de renseignements sont souvent en mesure de les retracer plus rapidement et facilement que les organismes d'application de la loi. Une ordonnance de production peut aussi permettre d'obtenir

[18] Le coût du nouvel équipement et de la mise à niveau de l'ancien.

des renseignements qui sont sous le contrôle mais non en la possession de tierces personnes, notamment des données stockées à l'extérieur du Canada.

2. Les techniques d'enquête de nature préliminaire sont souvent utilisées pour résoudre des affaires criminelles. Le recours à une ordonnance de production par laquelle un juge[19] autoriserait le contrôle des transactions effectuées pendant une période de temps donnée est une proposition logique et sensée qui est compatible avec la législation en vigueur[20]. Il représente un compromis raisonnable entre l'obligation d'obtenir un mandat de perquisition pour obtenir des renseignements de nature plus confidentielle et le libre accès à l'information sans aucune autorisation judiciaire.

3. Les mandats de perquisition ne devraient être requis que pour obtenir des renseignements plus personnels ou intimes au sujet de la personne visée dans le mandat[21].

4. Les ordonnances de production devraient être rendues par un juge qui est convaincu d'une part, que l'enquêteur, ayant fait une déclaration sous serment (ou une déclaration solennelle) à cet effet, exécute de bonne foi une tâche autorisée par la loi et d'autre part, que l'ordonnance est raisonnablement nécessaire pour mener cette tâche à terme.

H. ORDONNANCES SPECIFIQUES DE PRODUCTION DE DONNEES SUR LE TRAFIC

1. Il n'y a aucune disposition actuellement dans le *Code criminel* traitant de la collecte de données sur le trafic. Il faudrait créer une ordonnance de production spécifique pour l'acquisition de données relatives au trafic que l'on pourrait obtenir un peu comme on le fait avec les enregistreurs de numéro de téléphone (ENT).

2. La définition de données sur le trafic que l'on retrouve dans le document de consultation, soit des « données relatives aux télécommunications», devrait être retenue dans le projet de loi.

3. L'article 492.2 *du Code criminel* devrait être modifié pour permettre l'acquisition d'ENT et de données sur le trafic lorsqu'on a des raisons raisonnables de croire que les renseignements obtenus pourraient permettre aux organismes d 'application de la loi d'empêcher qu'une personne ne soit blessée ou tuée, même s'il ne s'agit pas d'une enquête sur la perpétration d'un acte criminel.

I. ORDONNANCES SPECIFIQUES DE PRODUCTION DE RENSEIGNEMENTS SUR LE NAA ET L'IFSL

1. Il est essentiel, tant pour mener les enquêtes que pour constituer la preuve, d'avoir des renseignements fiables et accessibles sur les abonnés. Les autorités doivent être en mesure d'identifier le propriétaire d'un compte ou service.

2. Le nom et l'adresse de l'abonné et l'information sur le fournisseur de services local (NAA/IFSL) ne sont pas des renseignements personnels et une autorisation du tribunal ne devrait pas être nécessaire pour les obtenir. Cependant, les fournisseurs de services de communication ne sont pas tenus à l'heure actuelle d'acquiescer à une demande de production de cette information. Il y aurait lieu d'inclure dans la loi une disposition obligeant les FSC à fournir ces renseignements aux organismes d'application de la loi et de sécurité nationale. Si cette suggestion est rejetée pour des motifs ayant trait au respect de la vie privée, il y aurait alors lieu d'envisager l'établissement d'une ordonnance de production assujettie à des règles simplifiées.

3. Les renseignements sur le NAA et l'IFSL sont essentiels pour que les organismes d'application de la loi puissent remplir leur rôle et pour que le Canada puisse respecter ses engagements internationaux en matière de coopération. Les fournisseurs de services de communication devraient être tenus de conserver ces données comme condition préalable à l'autorisation de mener des affaires au Canada. Le fait qu'ils doivent faire face à la concurrence ne doit pas les soustraire à l'obligation d'agir de manière responsable socialement.

---

[19] Le mot « juge » dans le présent rapport s'entend également de « juge de paix ».
[20] Art. 487.01 et par. 529(1) du *Code criminel* et *R. v. Noseworthy* (1997) 33 O.R. (3d) 641 (C.A. Ont.) – cité par un répondant.
[21] *R. c. Plant* (1993) 3 R.C.S. 281 – citée par un répondant.

4. Une base nationale de données pourrait être créée dans laquelle les fournisseurs de services de communication verseraient les données sur le NAA et l'IFSL et à laquelle pourraient accéder les organismes d'application de la loi et de sécurité nationale. Elle pourrait être dirigée et mise à jour par une société privée choisie à la suite d'un appel d'offres comme en Australie ou peut-être par un partenariat public/privé.

5. Subsidiairement, un système de distribution de données pourrait être mis en place permettant aux demandes des organismes d'application de la loi d'être automatiquement acheminées aux bases de données des services de communication par un mécanisme intermédiaire. Les réponses leur seraient retournées par la même voie. Quel que soit le système choisi, il faudrait prévoir des mesures de sécurité pour interdire l'accès non autorisé.

6. Le financement du système choisi relèverait du gouvernement fédéral.

J. ORDONNANCES D'ASSISTANCE

1. Les juges peuvent déjà rendre des ordonnances d'assistance en vertu de l'article 487.02 *du Code criminel*. Cet article devrait cependant être modifié pour s'appliquer également aux ordonnances de production.

K. ORDONNANCES DE CONSERVATION DES DONNEES

1. Les formes électroniques de preuve sont en soi volatiles et il faut donc disposer d'un mécanisme garantissant que la preuve ne sera pas perdue ou détruite avant que les autorités n'aient obtenu l'autorisation du tribunal d'en effectuer la saisie. La procédure pour obtenir une telle ordonnance devrait être simplifiée et tenir compte du fait que l'atteinte à la vie privée est minime lorsqu'il s'agit simplement de demander à un tiers, comme un fournisseur de service Internet, de conserver des données qui existent déjà.

2. Si l'on établit un pouvoir d'ordonner à un fournisseur de services de conserver des données temporairement, cela ne veut pas dire que les organismes d'application de la loi pourront par la suite saisir les données sans satisfaire aux exigences requises pour obtenir une autorisation judiciaire, comme dans le cas de tout autre mandat de perquisition.

3. On devrait permettre aux enquêteurs ou à des représentants désignés des organismes d'application de la loi de rendre, dans des circonstances exceptionnelles, des ordonnances de conservation qui seraient valables pendant sept jours ouvrables. Pendant ce temps, les organismes d'application de la loi seraient tenus d'obtenir l'autorisation du tribunal pour prolonger l'ordonnance pendant une période maximale de 90 jours[22]. Lorsqu'il y des circonstances exceptionnelles, il faudrait avertir les fournisseurs de services de communication de la date et de l'heure à laquelle l'ordonnance de conservation sera signifiée.

4. Les ordonnances de conservation devraient s'appliquer à la fois aux données emmagasinées dans les ordinateurs et aux documents papiers.

5. Les ordonnances de conservation doivent être rendues par un juge qui est convaincu que l'enquêteur visé, sur la foi d'une déclaration assermentée (ou déclaration solennelle) de sa part à cet effet, exécute de bonne foi une tâche autorisée par la loi et que l'ordonnance est raisonnablement nécessaire pour mener cette tâche à terme.

6. Il n'y a pas lieu que les normes juridiques soient différentes selon la nature des données à conserver. Celle-ci doit être prise en compte seulement au moment où un organisme d'application de la loi entend en faire l'acquisition, et non pour sa simple conservation par un fournisseur de services de communication ou autre gardien.

7. Les données devraient être conservées pour une période maximale de 90 jours, comme prévu dans la *Convention sur la cybercriminalité* – sous réserve de prolongation accordée par les tribunaux pour des motifs valables.

[22] Voir le précédent créé par l'article 487.11 et le par. 529.3(1) du *Code criminel* – cité par un répondant.

8. Les infractions actuelles d'entrave à la justice et de désobéissance à une ordonnance du tribunal contenues dans le *Code criminel* et l'infraction en common law d'outrage au tribunal sont suffisantes pour sanctionner le non-respect délibéré d'une ordonnance de conservation.

L. PROPAGATION DES VIRUS

1. Il faut protéger l'infrastructure de l'Internet contre les attaques malveillantes et destructrices par l'adjonction au *Code criminel* d'infractions de possession, de création ou de vente de virus, sans motif légitime.

2. La législation canadienne doit être intransigeante et conforme aux lois comparables dans d'autres démocraties occidentales ainsi qu'à la *Convention sur la cybercriminalité*.

M. INTERCEPTION DU COURRIER ELECTRONIQUE

1. Les organismes canadiens chargés de faire appliquer la loi apprécient la proposition du gouvernement visant à clarifier les dispositions actuelles de la loi touchant l'interception et la saisie des courriels.

2. Les lois canadiennes actuelles s'appliquant à l'interception et à la saisie du courrier électronique créent de la confusion et doivent être clarifiées. L'accès au contenu d'un courriel et sa saisie doivent toujours être assujettis à l'autorisation préalable d'un juge. Toutefois, la saisie de ce matériel ne semble pas rencontrer la définition ou les exigences procédurales de l'interception. Un courriel est plutôt assimilable à une lettre envoyée par la poste et devait être saisi en vertu des dispositions relatives au mandat de perquisition du *Code criminel*.

3. Il y aurait lieu d'ajouter une disposition spécifique au *Code criminel* portant sur l'interception d'un courriel sur ordonnance du tribunal.

4. Le stade de la transmission d'un courriel ne devrait pas être une considération pertinente pour déterminer le type d'ordonnance requise pour l'intercepter. De plus, les critères procéduraux plus sévères qui s'appliquent à l'interception des communications vocales ne devraient pas s'appliquer à l'interception du courrier électronique.

5. Les personnes qui conversent au téléphone, conventionnel ou cellulaire, peuvent raisonnablement conclure qu'aucune copie ne sera faite de leur conversation. On ne peut pas en dire autant des communications par courrier électronique sur Internet. Un courriel est en texte qui passe souvent par plusieurs systèmes informatiques où des copies sont faites du message avant qu'il n'atteigne sa destination. Le degré de confidentialité auquel on peut raisonnablement s'attendre lorsqu'on utilise le courrier électronique ne serait donc pas le même que lorsqu'on utilise des moyens transitoires de communication vocale, avec ou sans fil.

N. AUTRES SUJETS ABORDES PAR LES REPONDANTS

Surveillance vidéo

1. Le par. 487.01(4) du *Code criminel* a fourni à la police un outil précieux dans le cadre de la lutte contre les crimes graves, mais il exige que la surveillance vidéo soit effectuée exclusivement par des policiers, ce qui grève lourdement les ressources existantes de la police.

2. Des civils bien formés qui effectuent déjà des interceptions visées par la Partie VI du *Code criminel* peuvent facilement s'acquitter de la surveillance vidéo.

3. Il faudrait modifier le par. 487.01(4) du *Code criminel* pour permettre non seulement aux agents de la paix, mais à toute personne agissant sous son autorité, d'effectuer de la surveillance vidéo.

Communications ciblées

4. Les ordonnances d'interception rendues par le tribunal en vertu de la Partie VI du *Code* doivent indiquer le lieu où les communications peuvent être interceptées. Cette approche ne présentait aucun problème quand la plupart des interceptions se faisaient sur des lignes téléphoniques conventionnelles, mais elle ne s'applique pas de nos jours aux services de communication sans fil extrêmement mobiles comme les téléavertisseurs bidirectionnels, le courrier électronique sans fil ou les téléavertisseurs numériques.

5. Certains organismes d'application de la loi sont d'avis qu'il faudrait modifier les alinéas 185(1)*e*) et 186(4)*c*) du *Code criminel* en remplaçant la mention du lieu de l'interception par une description des dispositifs[23] visés par l'interception.

6. D'autres proposent que l'on restructure les ordonnances d'interception pour autoriser l'interception des communications d'une personne en particulier plutôt que de celles transmises sur des pièces d'équipement que l'on croit être en la possession de cette personne. On souligne que la technologie actuelle permet couramment à une personne de se servir de nouveaux dispositifs et de cesser d'utiliser ceux qu'elle utilisait auparavant.

7. Quelle que soit la modification retenue, elle ne devrait pas s'appliquer aux mandats émis en vertu de la Partie VI autorisant de pénétrer dans un lieu pour y installer un dispositif d'écoute électronique, puisqu'il serait évidemment toujours nécessaire de donner une description de ce lieu.

Surveillance en direct

8. Les organismes d'application de la loi sont vivement préoccupés par les coûts de plus en plus élevés qu'ils doivent payer pour se conformer aux conditions s'appliquant à la surveillance en direct contenues dans la plupart des autorisations accordées en vertu de la Partie VI du *Code*.

9. La surveillance en direct exige qu'une personne autorisée écoute la communication privée à intercepter assez longtemps pour décider si celle-ci peut être interceptée légalement ou non. Si elle ne peut être écoutée en entier, il faut « laisser tomber » l'appel.

10. La surveillance automatique permet d'enregistrer toutes les communications privées effectuées sur un dispositif donné aux fins d'examen et d'analyse ultérieurs. La personne qui écoute l'enregistrement automatique est en mesure de « bloquer » une communication dont l'interception n'est pas autorisée, tout comme s'il s'agissait d'une écoute en direct. Le protocole de blocage d'appels conserve en mémoire un dossier, que le tribunal pourra consulter ultérieurement, identifiant les communications qui ont été écoutées par un organisme d'application de la loi et celles qui ne l'ont pas été.

11. Il y a lieu de modifier le *Code criminel* pour abolir l'exigence de la surveillance en direct lorsque l'organisme chargé de l'interception possède un dispositif de blocage d'appels.

Services prépayés ou facturés à l'utilisation

12. Les services cellulaires prépayés, les cartes d'accès Internet, les cafés Internet et les terminaux d'accès à Internet dans les bibliothèques publiques présentent tous des difficultés pour les organismes d'application de la loi parce que l'utilisateur du service peut facilement dissimuler son identité.

13. Conformément au principe selon lequel il ne faut pas créer de zones sures où l'interception ne serait pas possible, on devrait au Canada imposer par règlement l'identification des utilisateurs de services de communications prépayés au Canada et la tenue d'une base de données à jour sur les abonnés par le fournisseur de services.

[23] L'ACCP précise qu'une définition de « dispositif » devrait être ajoutée à la Partie VI du *Code*.

Interceptions transfrontalières

14. Plusieurs sociétés canadiennes de télécommunications sans fil et opérateurs de système de communications par satellite ont des aires de services qui chevauchent la frontière canado-américaine. Cela peut signifier que l'entité faisant l'objet d'une autorisation délivrée au Canada peut se trouver physiquement à Detroit, même si l'interception elle-même est effectuée au moyen d'un commutateur sans fil situé à Windsor.

15. Il y a lieu de modifier le *Code criminel* pour rendre légalement admissibles en cour les interceptions transfrontalières de communications sans fil ou par satellite, à la condition que l'interception vise un service de télécommunications situé au Canada.

16. Quand le fournisseur de services se trouve aux États-Unis et que l'entité visée par une autorisation délivrée au Canada se trouve au Canada, la situation devient plus difficile. Les seuls moyens qui existent actuellement pour obtenir des éléments de preuve aux États-Unis consistent à procéder par une commission rogatoire[24], autorisée par un tribunal, ou à invoquer un traité d'assistance juridique s'il en existe un. Il y a lieu de mettre en place de nouvelles procédures accélérées ou des accords permettant une assistance rapide. Il serait très utile aux organismes d'application de la loi des deux côtés de la frontière s'il existait un endroit central dans chaque pays où ces données pourraient être recouvrées.

Fournisseurs de services de communications sans infrastructure au Canada

17. Plusieurs sociétés qui offrent des services Internet aux Canadiens ont un bureau au Canada mais possèdent l'ensemble de leur infrastructure aux États-Unis. Ceci signifie qu'il est impossible de procéder à l'exécution d'une ordonnance d'interception au Canada.

18. On devrait légiférer afin d'obliger tous les fournisseurs de services de communication qui offrent des services aux Canadiens à disposer d'une capacité d'interception au Canada. Tout nouveau coût d'infrastructure auquel donnerait lieu le respect de cette exigence serait exclusivement assumé par le fournisseur de services.

Réseaux mobiles sans fil et services d'assistance numérique personnelle

19. Le réseau superposé de transmission de données à haute vitesse[25] tout récemment introduit par les fournisseurs de Services de communications personnelles (SCP) présente actuellement des difficultés en matière d'interception légale pour les organismes d'application de la loi. La situation se compliquera encore davantage avec l'arrivée des réseaux 3G mobiles sans fil à très haute vitesse.

20. De même, les téléavertisseurs et les assistants numériques personnels (PDA) peuvent être difficiles à intercepter sans l'étroite collaboration des fabricants, parce qu'ils emploient des algorithmes de marque déposée.

21. Il faut interdire aux fournisseurs de services de communication d'utiliser une technologie qui empêche l'interception légale, peu importe qu'ils aient fabriqué ou acheté cette technologie.

[24] Demande adressée par une autorité judiciaire à une autre autorité judiciaire de faire, dans son ressort, un acte d'instruction ou un autre acte judiciaire.

[25] Le GPRS (General Packet Radio Service) ou réseau de 2,5G. Il s'agit d'un service qui permet la transmission sans fil de données par paquets (ndt).

CHAPITRE 4 : COMMENTAIRES DES REPRESENTANTS DE L'INDUSTRIE

NOMBRE TOTAL DE MEMOIRES REÇUS : 19

Le nombre d'astérisques attribués à chaque commentaire indique la fréquence avec laquelle les répondants ont exprimé cette opinion ou une opinion semblable. Cinq astérisques signifient « très souvent ». Un astérisque signifie généralement qu'une seule réponse a porté sur le sujet, mais cette réponse peut avoir été fournie au nom d'une association ou d'un groupe représentant plusieurs organisations. La mention du groupe (ou des groupes) de répondants à la suite du commentaire signifie qu'au moins un répondant appartenant à ce groupe a exprimé cette opinion ou une opinion très semblable. On trouvera la liste des participants à l'annexe B.

Le sigle FSC utilisé dans le présent chapitre renvoie à des commentaires formulés par un ou plusieurs fournisseurs de services de communication suivants, ou l'une des associations qui les représentent :
Compagnies de téléphone – principales compagnies de téléphone à l'échelle nationale ou régionale, y compris les entreprises de circonscription locale ou inter-circonscription. (COTEL)
Fournisseurs de service Internet (FSI)
Fournisseurs de services sans fil (FSS)
Services fixes par satellite(SFS)

A. GENERALITES

1. Le document de consultation est trop vague et imprécis pour permettre autre chose que des commentaires très généraux. Il ne constitue pas la base d'une consultation significative. FSC, Banques[26] *****

2. Il faut procéder à d'autres consultations, et donner notamment une occasion de commenter les propositions précises contenues dans un avant-projet de loi avant son dépôt devant le Parlement. FSC, Banques *****

3. La plupart des fournisseurs de services qui ont répondu[27] appuient l'accès légal et acceptent que les organismes canadiens d'application de la loi et de sécurité nationale puissent légalement intercepter des communications, compte tenu des changements technologiques, sous réserve de la protection accordée aux Canadiens par la *Charte canadienne des droits et libertés*. FSC ****

4. L'interception du courrier électronique non ouvert et de communications numériques similaires en transit doit être considérée comme l'interception d'une « communication privée », et donc assujettie aux garanties offertes relativement à une autorisation sous le régime de la Partie VI du *Code criminel*. Pour avoir accès au courrier électronique qui a été ouvert et que l'usager a décidé de conserver, les organismes d'application de la loi devraient être tenus d'obtenir un mandat de perquisition ou une ordonnance de production. FSC, TI[28] ****

5. Le document de consultation n'a pas démontré que les dispositions actuelles de la loi ne permettent pas un accès efficace aux services de communication de données au Canada ou que des enquêtes et des poursuites ont échoué en raison d'une absence de capacité technique. FSC, TI ***

6. La loi proposée devrait concilier de façon impartiale le maintien des capacités d'accès légal avec la nécessité de fournir des services de télécommunications nouveaux et innovateurs au Canada, tout en améliorant l'efficience et la compétitivité du marché canadien. FSC ***

[26] Commentaires formulés par des représentants du secteur bancaire.
[27] Les autres n'avaient pas de commentaires à formuler sur cette question.
[28] Secteur des technologies de l'information. Contrairement aux autres représentants de l'industrie, le secteur des technologies comprend des fabricants de matériel et de logiciels de télécommunications.

7. L'industrie doit participer pleinement à la conception et à la mise en oeuvre des normes et exigences techniques pouvant être imposées par règlement. La formation d'un groupe de travail mixte réunissant le gouvernement et l'industrie pourrait s'avérer la meilleure solution. FSC **

8. Il n'y a aucune raison de précipiter l'adoption de cette loi aux dépens d'une consultation appropriée. Les normes techniques et le matériel requis ne seront sans doute pas disponibles avant plusieurs années et les organismes d'application de la loi ont exprimé leur satisfaction générale à l'égard des relations de travail qu'ils ont établies à ce jour avec les principaux fournisseurs de service Internet FSC **

9. La *Convention sur la cybercriminalité* du Conseil de l'Europe n'a pas été ratifiée par le Parlement canadien ; en fait, jusqu'à présent, seulement deux pays qui ont signé la convention à Budapest en 2001 l'ont ratifiée. Cet accord ne constitue donc pas une base solide pour justifier un élargissement de l'accès légal. FSC **

10. Les fournisseurs de services sans fil s'opposent à toute obligation qui pourrait entraîner l'élimination de certains services ou de certaines catégories de services, comme les services sans fil prépayés. FSC **

11. Le document de consultation ne prévoit pas de mesures de contrepoids pour protéger les intérêts du public et éviter l'utilisation abusive des pouvoirs proposés. FSC **

12. Les fournisseurs de services sans fil sont actuellement régis par les 23 normes du Solliciteur général, qui renvoient à l'interception des communications téléphoniques à fil du type prévu dans la CALEA[29]. Les fournisseurs de services sans fil se préoccupent grandement de la possibilité que ces mêmes normes soient appliquées à des services offerts par la commutation de paquets. Les membres de l'industrie désirent obtenir des précisions sur ce qui adviendra des conditions actuelles de leur licence et de ces normes lorsque la nouvelle loi entrera en vigueur. FSC *

13. La position du gouvernement quant à la rétention des données et au traitement du trafic de données encodées n'est pas exposée dans le document de consultation. Ces questions sont trop importantes pour qu'on n'en tienne pas compte. TI *

B. OBLIGATION DE GARANTIR LA CAPACITE D'INTERCEPTION

1. L'expression « installation de télécommunications » n'est pas définie dans le document de consultation (même si elle est utilisée plusieurs fois dans le texte). Certaines définitions fournies dans le document de consultation diffèrent de celles qui sont données dans la *Loi sur les Télécommunications*. Des définitions claires et compatibles avec celles utilisées sur le plan international sont essentielles au succès de la loi proposée. FSC ***

2. L'ajout à l'intérieur d'un réseau d'une seule nouvelle pièce d'équipement assorti d'une capacité d'interception accrue ne devrait pas entraîner pour le fournisseur de services l'obligation d'améliorer l'ensemble de ce réseau. FSC ***

3. Les fabricants de logiciels permettant l'accès légal exigent à la fois l'installation du logiciel en question et l'achat d'un « droit d'utilisation », (ce qui peut s'avérer coûteux), avant d'activer certaines fonctions. Les fournisseurs de services ont fait la suggestion suivante : la loi proposée devrait exiger que ces fabricants maintiennent la capacité logicielle générale et qu'ils n'activent certaines fonctions particulières nécessitant des droits d'utilisation que lorsqu'ils reçoivent une demande d'utilisation de ces fonctions des organismes d'application de la loi. FSC ***

4. Les banques canadiennes veulent avoir l'assurance qu'elles ne seront pas considérées comme des *fournisseurs de services* aux termes de la loi proposée parce qu'elles exploitent de vastes réseaux de communications et des installations connexes. La même question se pose pour un certain nombre d'entreprises privées, d'hôtels, d'universités et de ministères. Banques, TI ***

[29] *Communications Assistance for Law Enforcement Act* (Loi sur l'aide des services de communications à l'application de la loi) - adoptée en 1994 par le Congrès américain.

5. Certains FSC soulignent que lorsque de petits exploitants (comme les cafés Internet) offrent des services concurrentiels au public, ils devraient être désignés comme étant des fournisseurs de service dans la nouvelle loi. FSC ***

6. Les fournisseurs de services ne devraient pas être obligés de formuler des solutions à des questions d'accès légal touchant des services ou des technologies lorsque les vendeurs n'en ont pas encore, car les coûts pourraient être exorbitants. FSC ***

7. Les fournisseurs de services ne devraient pas être tenus de fournir un accès légal aux systèmes et aux données de réseau qu'ils utilisent aux fins de la prestation de leurs services, mais dont la propriété et le contrôle relèvent d'autres entreprises. FSC ***

8. Tous les fournisseurs de services qui se font concurrence sur le même marché devraient être assujettis à des exigences semblables en matière d'accès légal, qu'il s'agisse de fournisseurs dotés d'installations, de revendeurs ou de tiers fournisseurs. Les règlements ou les normes doivent être suffisamment souples pour s'adapter aux différentes technologies utilisées par les entreprises de télécommunications en question. FSC **

9. Les grands fournisseurs de services ne devraient pas être chargés de fournir l'infrastructure ou une assistance opérationnelle pour l'accès légal à des services de lignes privées ou à des services en gros, lesquelles devraient, juridiquement et financièrement, relever des fournisseurs de services à l'utilisateur final. FSC **

10. Les fournisseurs de services de communication par satellite sont mal placés pour fournir un accès légal utile et ne désirent nullement assumer les coûts à cet égard. Ils agissent à titre de transporteurs de télécommunications pour des entreprises offrant des services téléphoniques et Internet. En général, ils ne possèdent aucune installation au sol faisant partie de ces réseaux. Selon eux, la meilleure surveillance est exercée auprès des fournisseurs de services aux utilisateurs finals (comme les fournisseurs de service Internet) et des installations au sol des entreprises de télécommunications, ce qui est traditionnellement le cas. FSC *

11. Les fournisseurs de services qui utilisent le cryptage dans leur réseau devraient pouvoir décider de fournir une clé ou de livrer un texte non encodé, sur demande d'un organisme d'application de la loi. TI *

12. On devrait définir l'« amélioration significative » comme étant le remplacement ou une modification majeure de l'ensemble des logiciels et du matériel utilisés par le réseau central du fournisseur de services. FSC *

13. L'expression « réseau central » devrait désigner toute entité physique qui fournit un soutien aux fonctions de réseau et aux services de télécommunications, y compris une entité qui fournit de l'information sur l'emplacement des abonnés ainsi que des services de supervision de réseau, de commutation et de transmission. FSC *

C. REGLEMENTS

1. La plupart des FSC conviennent qu'il est crucial de savoir et de comprendre ce que les organismes d'application de la loi attendent d'eux. FSC ****

2. Les fournisseurs de services s'opposent à l'établissement d'exigences propres au marché canadien relatives à l'accès légal. Selon eux, il est très peu probable que les fabricants de matériel de télécommunications mettent au point des dispositifs d'interception de communications par Internet ou sans fil, spécialement pour le marché canadien. S'ils le font, ces dispositifs seront très probablement coûteux et ils en seront les propriétaires. FSC ****

3. Qu'entend-on par « exigences fonctionnelles générales » et « capacité de base d'interception »? Les capacités actuellement offertes aux organismes d'application de la loi seront-elles conformes à la norme? Qu'en est-il des spécifications d'interface? FSC ***

4. Les normes techniques pour l'accès légal devraient être établies par des spécialistes de l'industrie et approuvées par des groupes de travail regroupant l'industrie et le gouvernement. Dans la mesure où il offre la capacité d'interception requise, le fournisseur devrait pouvoir aménager le réseau pour y arriver. FSC, TI ***

5. En bout de ligne, ce sont les fabricants qui devraient avoir la responsabilité de créer du matériel conforme. Toute solution standard qui satisfait aux exigences de la loi américaine devrait être ainsi considérée au Canada. FSC, TI ***

6. Certaines entreprises ont engagé des frais de personnel et des frais indirects élevés en répondant à des demandes d'accès légal, qu'ils ont eu du mal à recouvrer. Il devrait être précisé clairement dans les règlements ou dans la loi elle-même qu'une indemnisation raisonnable est payable à titre d'aide opérationnelle (voir F2 plus loin). FSC **

7. Outre la mention à l'effet d'obtenir les autorisations de sécurité pertinentes, les règlements ne devraient pas établir de normes quant à la compétence, la fiabilité et la mise en place du personnel du fournisseur de services. Cette responsabilité devrait revenir à l'employeur. FSC **

8. Il faudrait exiger que le matériel de communication vocale ou de transmission de données, dont l'utilisation sur le marché canadien des télécommunications est envisagée, puisse offrir un accès légal. FSC *

9. Le règlement est une forme d'application du droit qui n'est pas soumise au même niveau d'examen du public que la loi. FSC *

10. Des questions comme la distribution des coûts, les normes techniques et opérationnelles et les obligations du fournisseur de services découlant d'une ordonnance d'interception sont bien trop importantes pour l'industrie pour être régies par voie réglementaire et mériteraient plutôt d'être assujetties à un examen parlementaire exhaustif. FSC *

D. EXEMPTION

1. Il y a lieu de définir des critères d'exemption qui soient clairs et uniformes. Toute règle ou norme relative à l'exemption devrait être équitable et transparente. FSC ***

2. L'exemption peut créer pour des criminels des zones sûres identifiables où l'interception ne serait pas possible. FSC ***

3. Certains fournisseurs de services sans fil ont dit que tout fournisseur de services incapable de fournir une capacité minimale d'interception devrait être tenu de demander une exemption. D'autres ont indiqué que les fournisseurs de services devraient pouvoir demander d'être exemptés de toute obligation qu'ils ne peuvent raisonnablement pas satisfaire. FSC **

4. Les représentants de l'industrie devraient participer à l'élaboration de lignes directrices administratives régissant le traitement des demandes d'exemption. **

5. Bien que l'exemption soit nécessaire pour l'évaluation de services expérimentaux pour des périodes limitées, il n'est pas certain qu'une politique d'exemption générale s'impose. Des solutions d'interception sont disponibles pour pratiquement tous les services de télécommunications publiques actuellement en usage. TI *

6. Aucun régime d'exemption ne devrait désavantager concurrentiellement les fournisseurs qui se conforment à la loi par rapport à ceux qui ne s'y conforment pas. FSC *

E. MECANISMES DE CONFORMITE

1. Il faut communiquer aux fournisseurs de service Internet des lignes directrices claires et des procédures à suivre lorsqu'ils reçoivent signification d'une ordonnance judiciaire FSC **

2. Les grands fournisseurs de services suggèrent que leur conformité devrait être déterminée en fonction des résultats de leur coopération régulière avec les organismes d'application de la loi et de sécurité et que les petits fournisseurs fassent l'objet d'inspections d'application de la loi par le Solliciteur général. Demander à chaque organisme d'application de la loi ou de sécurité nationale de mener ses propres inspections constituerait probablement une approche irréalisable. FSC **

3. Certains fournisseurs de services s'opposent fermement à un système faisant appel à des inspections périodiques ou aléatoires pour déterminer la conformité ou à un système leur demandant d'enregistrer leur conformité, pour des raisons de coût. De plus, cette solution entraînerait une augmentation de la paperasserie. FSC **

4. L'outrage au tribunal constitue un moyen dissuasif efficace contre le défaut de se conformer à un mandat, à une ordonnance de production, etc. L'infraction punissable par voie de déclaration sommaire de culpabilité s'avère parfois nécessaire pour régler les cas persistants et injustifiés de non conformité aux exigences relatives à la capacité d'accès légal. FSC **

5. Des sanctions ne devraient être imposées que si un fournisseur de services est incapable ou refuse de respecter ses obligations lorsqu'il reçoit signification d'une ordonnance judiciaire rendue en bonne et due forme. FSC *

6. Tout nouveau régime devrait être fondé sur le modèle que l'on utilise avec succès au Canada depuis 1996 pour effectuer le suivi en matière de la conformité des titulaires de licence de services de communications personnelles. FSC *

F. COUTS

1. Les fournisseurs de services ne devraient pas avoir à payer pour l'établissement de la capacité de base d'interception, quelle que soit la façon dont les expressions « amélioration significative » et « nouveau service ou nouvelle technologie » sont définies dans la loi. Jusqu'à ce que des solutions techniques soient disponibles relativement à l'équipement de transmission utilisé par les fournisseurs de services, susceptibles d'être mises en place et appliquées moyennant un coût additionnel minime pour le fournisseur de services, le gouvernement devrait assumer les coûts au titre de la « capacité de base d'interception » (quelle que soit la définition donnée à l'expression). FSC, TI *****

2. La loi devrait faire en sorte que les organismes d'application de la loi demeurent responsables des coûts raisonnables engagés par les fournisseurs de services qui leurs offrent une aide opérationnelle aux fins de l'exécution d'ordonnances légitimes d'interception, de saisie et de conservation. Ces coûts devraient être négociés entre chaque fournisseur de services et l'organisme visé, au lieu d'être fixés selon des tarifs universels établis dans les règlements pour les divers types d'aide. Industrie Canada et le Solliciteur général devraient arbitrer les différends au sujet des frais de services entre les fournisseurs de services et les organismes d'application de la loi. FSC, TI *****

3. La prestation de services d'accès légal aux organismes d'application de la loi engendre des coûts permanents élevés sur le plan du personnel, de la formation et de la sécurité, qui s'ajoutent aux coûts de la mise en oeuvre d'une capacité d'interception. FSC ****

4. Le coût des mises à niveau des nouvelles technologies et du maintien de l'accès à ces technologies pour les organismes d'application de la loi au Canada correspond à une taxe gouvernementale sur l'innovation technique par les fournisseurs de service Internet. S'ils ne sont pas remboursés par le gouvernement, ces coûts devront être refilés aux consommateurs, ce qui réduit la compétitivité et constitue une puissante mesure dissuasive contre l'innovation technologique et l'investissement par les fournisseurs de service Internet canadiens. FSC, TI ***

5. Il faut veiller à ce que l'obligation de fournir la capacité d'accès légal ne crée un gain fortuit pour les fabricants de matériel de télécommunications. Il est inéquitable que les fournisseurs de services soient assujettis à un recouvrement des coûts lorsqu'ils fournissent une assistance aux organismes d'application de la loi, et que les fabricants de matériel ne soient assujettis à aucune restriction de prix lorsqu'ils vendent aux fournisseurs de services le matériel et les logiciels nécessaires pour fournir la capacité d'accès légal. FSC ***

6. L'accès légal est exigé dans l'intérêt du public et son coût devrait en être assumé par l'ensemble des contribuables canadiens. FSC ***

7. En l'absence d'argument à l'effet que les FSC sont aux prises avec un fardeau financier injustifié, le coût pour fournir l'accès légal devrait être assumé par l'industrie à titre de devoir civique. FSC *

8. Le coût élevé que devraient subir les petits fournisseurs de services pour se conformer aux exigences proposées en matière de capacités d'interception et pour maintenir ces capacités pourrait leur causer un préjudice financier grave et irréparable. FSC *

9. Si les fournisseurs de services étaient malgré tout obligés par la loi proposée d'assumer, en bout de ligne, les coûts de l'accès légal, la loi devrait prévoir que tous les fournisseurs de services, y compris ceux dont les tarifs sont réglementés, puissent recouvrer ces coûts additionnels de leurs clients. FSC *

G. ORDONNANCES GENERALES DE PRODUCTION

1. Il faudrait accorder aux fournisseurs de services un délai raisonnable pour répondre à une ordonnance de production selon la nature des données, le nombre de sources à perquisitionner et les installations disponibles pour effectuer ces perquisitions. FSC **

2. La définition de « données relatives aux télécommunications » fournie dans le document de consultation devrait être modifiée par l'ajout de la phrase suivante à la suite de la dernière phrase : « et qui ne révèlent pas, directement ou indirectement, de détails importants quant au contenu de la transmission. » FSC *

3. Les instruments juridiques autorisant l'accès devraient être des ordonnances de la Cour supérieure; l'approbation par un juge de paix ne constitue pas une garantie suffisante. TI *

4. Les fournisseurs de services s'opposent aux « ordonnances anticipatoires », car elles semblent obliger un possesseur à produire des documents qu'il n'a pas encore en sa possession et dont il n'aurait probablement pas la possession dans le cours normal de ses activités. FSC *

5. La nouvelle loi devrait contenir des dispositions visant à protéger les fournisseurs de services contre toute poursuite civile ou criminelle lorsqu'ils se conforment aux conditions d'une ordonnance judiciaire. L'article 25 du *Code criminel* ne fournit pas une protection suffisante dans tous les cas. FSC *

6. Le document de consultation fait mention de perquisitions chez des possesseurs tiers, comme une banque ou une société, où la banque ou la société effectue la perquisition au nom de l'organisme d'application de la loi dans un délai convenu. Les fournisseurs de service Internet désirent savoir si ce type d'ordonnance de production pourrait s'appliquer à eux. Pour eux, il n'est pas clair si un paquet IP peut devenir un document ou à quel stade de la communication d'un message électronique le fournisseur de service Internet pourrait devenir un possesseur. FSC *

7. L'utilisation du terme « document » dans un contexte de réseau de communication de données peut engendrer de la confusion et devrait être clarifiée. Il est évident que les courriels et les pièces jointes à des courriels sont des documents, mais que dire des pages Web, du trafic d'égal à égal, des messages en temps réel à relais instantané et des fichiers journaux? TI *

8. Selon le document de consultation, les ordonnances de production faciliteront la saisie des documents stockés dans un État étranger. Cependant, on n'y examine pas ce qui arrive si l'État étranger n'acquiesce pas à l'ordonnance ou si le Canada reconnaîtra les ordonnances de production rendues à l'étranger. TI *

9. S'il est probable que les données d'enquête seront communiquées à l'extérieur du territoire, l'instrument juridique autorisant la surveillance devrait être approuvé par un juge de la Cour supérieure. TI *

H. ORDONNANCES SPECIFIQUES DE PRODUCTION POUR LES DONNEES RELATIVES AU TRAFIC

1. Les « données relatives aux télécommunications » Internet peuvent s'avérer plus menaçantes pour la vie privée que les données équivalentes relatives aux services téléphoniques. Ainsi, les enregistrements des moteurs de recherche Internet peuvent avec le temps révéler des renseignements personnels intimes. L'interception de ce type de renseignements devrait faire l'objet d'une surveillance judiciaire. De plus, la définition du terme « données relatives au trafic » devrait être interprétée de manière restrictive, comme c'est le cas dans la *Convention sur la cybercriminalité*[30]. FSC, TI ****

2. Toutes les garanties procédurales qui s'appliquent actuellement aux ordonnances d'interception devraient être maintenues dans les cas où il y a possibilité que les données portent sur le contenu d'une communication ou donnent accès à une communication ou encore puissent être utilisées ou manipulées pour déterminer ou suggérer le contenu d'une communication. FSC ***

3. Les ordonnances de conservation et de production ne devraient s'appliquer qu'à des données qui sont clairement sous le contrôle des fournisseurs de services de télécommunications et non à des données qui sont gérées par les utilisateurs, même si elles se trouvent sur les installations des fournisseurs de services. FSC **

4. Certains fournisseurs de service Internet sont en faveur de l'utilisation d'un critère moins exigeant pour la production de données relatives aux télécommunications et de renseignements sur le NAA, comme c'est le cas pour l'accès légal aux données relatives aux services téléphoniques. FSC *

I. ORDONNANCES SPECIFIQUES DE PRODUCTION DE DONNEES SUR LE NAA ET L'IFSL

1. On s'oppose fortement à ce que les fournisseurs de services soient obligés de recueillir et de tenir à jour des renseignements sur les abonnés autres que ceux dont ils ont besoin pour leurs fins commerciales, et de garantir l'exactitude de ces renseignements. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ) limite la collecte de renseignements personnels inutiles et leur conservation pour des périodes dépassant les besoins normaux de l'entreprise. Les fournisseurs de services ne sont pas des organismes d'application de la loi et la nouvelle loi ne devrait pas leur attribuer cette fonction. FSC, TI *****

2. Les fournisseurs de services sont aussi fortement opposés à la création de toute base de données pancanadienne sur leurs abonnés, invoquant des motifs liés à la protection de la vie privée et à la sécurité, ainsi que le coût élevé associé à la création et à la mise à jour d'une telle base de données. Ils font remarquer que la plupart des cybercriminels sont tout à fait capables d'utiliser de faux noms, des comptes piratés ou des terminaux d'accès publics pour leurs communications ou transactions. FSC ****

3. S'il est établi que la base de données des noms et adresses des abonnés (NAA) d'un fournisseur de services est nécessaire, son exploitation pour les fins d'application de la loi devrait être coordonnée par un tiers indépendant de l'organisme d'application de la loi et du fournisseur de services. La base de données de chaque fournisseur de services devrait contenir le nom et l'adresse des abonnés associés uniquement au service téléphonique à fil. FSC *

J. ORDONNANCES D'ASSISTANCE

1. Les fournisseurs de services sont tout à fait en faveur des ordonnances d'assistance qui exposent clairement et de façon précise ce que l'on attend d'eux. FSC ***

2. Certains grands fournisseurs de services soutiennent qu'ils connaissent leur réseau bien mieux que tout organisme d'application de la loi ne le connaîtra jamais et ils sont disposés à offrir leur aide à l'exécution de mandats ou d'ordonnances sans qu'il soit nécessaire que la loi les y oblige. FSC **

[30] « Toute donnée ayant trait à une communication passant par un système informatique, produite par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent. » Chapitre 1, Article 1(d), cité par un répondant.

K. ORDONNANCES DE CONSERVATION DES DONNEES

1. Les fournisseurs de services ont exprimé une forte opposition à toute obligation de stockage des données en raison des répercussions sur le coût et la dotation en personnel, et des exigences techniques importantes à l'endroit des réseaux. Des limites raisonnables devraient être imposées quant à la quantité de données à saisir, à stocker et à livrer aux termes d'une ordonnance de conservation. FSC ***

2. Les grands fournisseurs de services sont généralement d'accord avec l'introduction des ordonnances de conservation dans le droit canadien, à condition qu'elles soient explicites et non ambiguës, bien ciblées et de courte durée, et qu'elles accordent aux fournisseurs de services un délai raisonnable pour s'y conformer. FSC **

3. La notion d'ordonnances de conservation rendues dans des « circonstances exceptionnelles » sans autorisation judiciaire est également acceptable pour les grands fournisseurs, à condition que les données ne soient conservées que pendant la période nécessaire pour obtenir une ordonnance de la cour, soit un délai qui ne devrait pas dépasser quatre jours. Une « demande exceptionnelle » pleinement fondée devrait être assortie d'une restriction explicite quant à la responsabilité du fournisseur de services. FSC **

4. La période de conservation ne devrait pas dépasser 90 jours, comme l'exige la *Convention*. Si les organismes d'application de la loi exigent l'isolation, le filtrage ou l'interception possibles de données, plutôt qu'un simple stockage de données brutes pour une période limitée, l'ordonnance devrait être assujettie à la norme d'autorisation judiciaire la plus élevée. FSC **

5. Selon un rapport du G8[31], la conservation des données n'oblige ni la collecte ni le stockage des données; il s'agit simplement d'une ordonnance d'« interdiction de suppression » touchant les données existantes. On présume qu'un fournisseur de service Internet donné effectue déjà la collecte des données visées, sinon il n'y aurait aucune donnée à conserver. En pratique, les fournisseurs de service Internet ont très peu souvent besoin de recueillir ou de stocker des données relatives au trafic. FSC, TI **

6. En général, la demande d'ordonnance de conservation des données est présentée dans l'intention d'obtenir ultérieurement une autre ordonnance, comme une ordonnance de production ou un mandat de perquisition. Les organismes d'application de la loi devraient donc être tenus de faire la preuve qu'ils sont susceptibles d'obtenir cette autre ordonnance avant que l'ordonnance de conservation ne soit autorisée. Banques *

7. Il devrait être clairement précisé dans la loi que les données conservées aux termes d'une ordonnance de conservation ne seront accessibles qu'à l'organisme dûment mandaté pour les fins d'application de la loi ou de sécurité nationale. Elles ne seront pas disponibles pour les organismes ou les autres personnes qui désireraient y avoir accès pour toute autre fin ou procédure judiciaire, comme l'assignation à témoigner. FSC *

8. L'ordonnance de conservation des données devrait être assujettie aux mêmes critères judiciaires que le mandat de perquisition, pour que les organismes d'application de la loi ne l'utilisent pas à la légère. FSC *

L. PROPAGATION DES VIRUS INFORMATIQUES

1. La loi devrait exiger que les organismes d'application de la loi prouvent l'existence d'une intention criminelle pour établir qu'il y a eu perpétration d'une infraction. Cette distinction est importante pour les laboratoires de logiciel, les fournisseurs de services, les entreprises de télécommunications et les spécialistes de la sécurité dont les fonctions exigent qu'ils soient en possession de virus informatiques à des fins de tests légitimes. FSC, TI ***

2. La loi devrait préciser clairement que les fournisseurs de services ne seront pas tenus responsables s'ils ignoraient tout de l'existence de virus sur leurs réseaux. FSC, TI ***

[31] Listes de contrôle sur la préservation des données (http://www.gj-i.ca/french/doc4).

M. INTERCEPTION DU COURRIER ELECTRONIQUE

1. Le critère pour établir s'il y a accès légitime au courrier électronique[32] consiste à vérifier si le message a été reçu (lu ou vu) par le destinataire prévu. Si le message n'a pas été reçu (introduit par clavier, non envoyé, non arrivé, non ouvert, etc.), il devrait être considéré comme une « communication privée » en transit et être soumis à la même obligation de fournir l'accès légal que les activités d'écoute électronique visées par l'article 186 du *Code criminel* . FSI, COTEL, TI *****

2. La loi doit préciser clairement à quel stade de la transmission d'un courriel l'interception ou la saisie devrait se faire et comment on devrait procéder. FSI **

3. Les utilisateurs du clavardage, de SEMC[33] et d'autres services semblables ont des attentes raisonnables en matière de vie privée, étant donnée la nature transitoire de leurs communications. La définition de « communication privée » devrait être élargie pour englober explicitement ces autres services ainsi que le courrier électronique. FSC **

4. Les attentes en matière de vie privée sont moins élevées lorsqu'il est question de matériel stocké, puisqu'il peut être vu et distribué à d'autres personnes. Un mandat de perquisition ou une ordonnance de production devrait être obligatoire pour obtenir l'accès légal à des communications stockées. FSC **

5. Les systèmes de courrier électronique ne font pas tous la distinction entre les courriels « ouverts » et « non ouverts ». Ainsi, dans certains systèmes, il peut arriver qu'il ne soit pas possible d'exécuter un mandat exigeant la saisie des courriels « ouverts » seulement. FSC *

N. MODIFICATIONS A LA *LOI SUR LA CONCURRENCE*

1. Généralement, on semble appuyer l'idée que le commissaire de la concurrence ait un accès, autorisé par un tribunal, aux dossiers cachés ainsi qu'un recours aux ordonnances d'assistance et de production en vertu des garanties contenues dans le *Code criminel*. FSC **

O. AUTRES SUJETS ABORDES PAR LES REPONDANTS

1. Certains répondants ont souligné la difficulté de concilier le droit fondamental du public à la vie privée et le besoin des organismes d'application de la loi d'avoir accès aux données qui leur permettront de mener efficacement des enquêtes criminelles et d'assurer la sécurité de l'État. Selon un certain nombre de répondants, la loi proposée pourrait bien faire pencher la balance du côté d'une intrusion abusive par les organismes d'application de la loi, à un tel point qu'il serait difficile de faire marche arrière. FSC **

[32] Et aux télécommunications de texte semblables.

[33] Services d'envoi de messages courts

CHAPITRE 5 : COMMENTAIRES DES COMMISSAIRES A LA PROTECTION DE LA VIE PRIVEE ET A L'INFORMATION DU CANADA

NOMBRE TOTAL DE MEMOIRES REÇUS : 5

A. GENERALITES

1. L'interception et la surveillance des communications privées constituent de graves atteintes à la vie privée des individus. C'est à ceux qui affirment qu'une nouvelle atteinte ou restriction au droit à la vie privée est nécessaire qu'il incombe d'en faire la preuve.

2. Toute mesure proposée en ce sens doit satisfaire au critère à quatre volets suivants :

- Il faut démontrer que la mesure proposée est nécessaire pour pouvoir répondre à un besoin précis
- Il faut démontrer qu'elle est susceptible de permettre d'atteindre efficacement l'objectif visé
- L'atteinte à la vie privée doit être proportionnelle aux avantages qu'elle comporte sur le plan de la sécurité
- Il faut démontrer qu'aucune autre mesure portant moins atteinte à la vie privée ne serait suffisante pour atteindre le même objectif

3. Les mesures proposées risquent de causer de la méfiance de la part du public à l'égard des technologies de l'information et des communications en général, en confirmant leur croyance qu'elles font constamment l'objet d'une interception ou du moins qu'elles sont susceptibles de l'être.

4. Les pouvoirs proposés pour accéder aux communications privées des Canadiens vont beaucoup plus loin que le maintien des capacités et des pouvoirs dont disposaient les organismes d'application de la loi et de sécurité nationale par le passé.

5. Le document de consultation ne renferme pas suffisamment d'éléments pour pouvoir conclure à l'existence de problèmes assez graves pour préconiser une solution qui passe par une telle immixtion dans la vie privée des Canadiens. Il s'ensuit qu'il n'est pas possible de savoir si les mesures proposées constituent une solution efficace et proportionnée au problème, en plus d'être la solution susceptible de porter le moins atteinte à la vie privée.

6. Il incombe aussi aux responsables de l'application de la loi de protéger la confidentialité de cette information, notamment lorsqu'il est démontré qu'elle n'a aucun rapport avec leurs enquêtes.

7. Les trois ministères qui ont participé à l'élaboration de la proposition devraient exposer clairement les problèmes auxquels ils sont confrontés, ainsi que des documents opérationnels étayant le besoin d'augmenter les pouvoirs d'interception et de surveillance proposés dans le document de consultation.

8. L'inquiétude au sujet de l'érosion inutile de la protection accordée à la vie privée devrait aller au-delà des propositions énoncées dans le document de consultation. Au cours de l'année écoulée, les Canadiens ont été confrontés à une série de lois susceptibles comme jamais auparavant de porter atteinte à leur vie privée : la loi antiterroriste, le projet de loi omnibus 42[34], et la création de la base de données sur les voyageurs aériens de l'Agence des douanes et du revenu du Canada. Cette législation a été introduite de manière fragmentée, sans que le contexte ne soit clairement articulé et à la suite de consultations et de discussions limitées.

9. Le respect de la vie privée est un droit protégé par la Constitution. La protection de la confidentialité des communications électroniques ne devrait céder le pas aux besoins des organismes d'application de la loi et de sécurité nationale que lorsque ces besoins l'emportent nettement sur le droit à la protection de la vie privée et, dans ce cas, seulement dans la mesure minimale nécessaire. Les dispositions actuelles du *Code criminel* relatives à

[34] Le projet de loi 42 est par la suite devenu le projet de loi 44 et le projet de loi 55 (maintenant C-17) – cité par un répondant.

l'interception des communications privées créent un juste équilibre entre le droit des particuliers à la protection de leur vie privée et le droit du public à une application efficace de la loi.

10. Le gouvernement du Canada ne devrait donner suite aux propositions formulées au sujet de l'accès que si la nécessité d'adopter les modifications proposées est clairement démontrée. Le gouvernement du Canada ne doit pas agir de la sorte simplement en raison du climat de peur et d'insécurité engendré dans la foulée des événements du 11 septembre 2001.

11. Il vaut la peine de signaler que l'Australie, l'Afrique du Sud et le Royaume-Uni ont récemment été témoins d'une forte opposition à l'adoption et à la mise en œuvre de nouvelles mesures législatives sur l'accès légal dont les objectifs étaient semblables à ceux qui sont exposés dans le document de consultation canadien.

12. Malgré une réglementation sévère et le fait que l'accès non autorisé au système sera sanctionné par la loi, le gouvernement ne pourra pas dans les faits empêcher les abus.

13. Les criminels s'apercevront rapidement qu'ils font l'objet de surveillance et utiliseront d'autres moyens de communication, tandis que la majorité des citoyens seront les victimes du système, incapables de débrancher tous leurs téléphones et autres moyens de communication.

14. Il n'est pas démontré que les lois actuelles en matière d'interception, de perquisitions et de saisies ne parviennent pas à traiter efficacement des communications électroniques modernes, ni que la *Convention sur la cybercriminalité* du Conseil de l'Europe offre une base solide pour les propositions. Celles-ci affaibliraient les protections actuelles en matière de respect de la vie privée au Canada sans justification claire et convaincante.

15. Les Canadiens ont le droit d'être assurés que leurs communications et activités en ligne ne seront pas arbitrairement interceptées et passées au peigne fin.

16. Le Canada n'a pas encore ratifié la *Convention*, de sorte que les obligations légales qui sont invoquées pour en faire appliquer les dispositions n'ont en réalité aucune existence.

17. Si la *Convention* autorise une violation injustifiable du droit à la vie privée des Canadiens qui serait incompatible avec nos valeurs et nos droits, le gouvernement canadien doit refuser de la ratifier.

18. Le gouvernement dans son document n'a pas démontré comment il respecterait l'article 15 – Conditions et sauvegardes – de la *Convention sur la cybercriminalité*, notamment comment il assurera une protection adéquate des droits de l'homme et des libertés et comment il respectera le principe de proportionnalité. Il y a d'ailleurs lieu de se demander comment l'application de la convention pourrait répondre à son propre article 15.

B. OBLIGATION DE GARANTIR LA CAPACITE D'INTERCEPTION

1. Toute nouvelle loi destinée à permettre l'interception et la saisie du contenu des communications sur Internet et des données relatives au trafic devrait avoir une portée aussi étroite et limitée que possible. On ne doit pas autoriser la surveillance électronique généralisée ou exploratoire. Des mesures législatives top vagues porteraient atteinte au droit à la vie privée et violeraient l'article premier de la *Charte des droits et libertés*.

2. Les nouvelles technologies et les nouveaux services de communications risquent fort de poser des problèmes en ce qui concerne les méthodes actuelles d'interception et d'obliger les FSC à assurer que leurs systèmes ont une capacité technique suffisante pour assurer un accès légal aux organismes chargés de l'application de la loi en matière d'interception et de surveillance.

3. Comme il est expliqué dans le document de consultation, ces capacités devraient servir à maintenir le statu quo et permettre une application efficace des pouvoirs actuels de l'État aux nouveaux services de communications. Autrement dit, les organismes d'application de la loi et de sécurité nationale devraient avoir la même capacité d'intercepter et de surveiller le courrier électronique et les communications par téléphone cellulaire, par exemple, que

celle dont ils disposent actuellement en ce qui concerne les envois postaux et les communications téléphoniques conventionnelles avec fil.

4. Avant que cette question ne puisse être raisonnablement évaluée, de plus amples renseignements devraient être communiqués sur la façon dont on procéderait à l'interception, sur les responsables de cette interception et sur les fins auxquelles elle serait effectuée; des propositions devraient aussi être présentées sur le niveau de preuve, les mesures de surveillance et les garanties.

5. En obligeant les fournisseurs de services à acquérir la capacité technique leur permettant d'offrir un accès légal, on contraint le secteur privé à faire de la surveillance pour le compte de l'État. Les coûts que les fournisseurs de services devront ainsi assumer se répercuteront sur les prix facturés aux consommateurs et risquent de nuire à la compétitivité des fournisseurs canadiens de services Internet. Le développement et la mise en application de la technologie Internet seront influencés par les intérêts des services de surveillance plutôt que par les besoins ou la réalité des entreprises canadiennes et de leurs clients.

6. L'interception de communications sur un système téléphonique traditionnel ne peut se comparer à la surveillance des systèmes de communications sans fil ou l'Internet car celle-ci peut fournir un plus grand nombre de renseignements personnels et être beaucoup plus envahissante. Il faut trouver une nouvelle approche pour traiter des nouvelles technologies, plutôt que de simplement prolonger les anciennes.

7. L'infrastructure, les outils et les bases de données qui seront nécessaires pour permettre l'accès légal tel que proposé exciteront la convoitise de plusieurs dont des organisations criminelles et des services d'espionnages de pays non signataires de la *Convention*. Dans ces cas, les auteurs de délits se gausseront des sanctions imposées à ceux qui violent les règles.

C. STOCKAGE DES DONNEES ET ORDONNANCES DE CONSERVATION

1. Le gouvernement doit continuer à refuser toute suggestion voulant que les exigences générales relatives au stockage des données fassent partie de l'initiative relative à l'accès légal.

2. Les ordonnances de conservation sont tout aussi dangereuses et mal adaptées du point de vue du droit à la vie privée que les ordonnances de stockage de données. Le concept d'ordonnance de conservation n'existe pas en droit canadien. L'affirmation suivant laquelle ce type de pouvoirs est nécessaire pour « maintenir » la capacité actuelle d'accès légal ne tient donc pas.

3. Le document de consultation ne permet pas de savoir avec certitude quel niveau de preuve de l'infraction soupçonnée devrait être respecté pour obtenir du juge qu'il prononce une ordonnance de conservation en faveur d'un FSC. Dans certains cas, il semble qu'aucune preuve ne serait nécessaire. L'ordonnance serait simplement émise par les organismes d'application de la loi et de sécurité nationale.

4. Le juge à qui l'on demande d'approuver une ordonnance de conservation peut être moins enclin à exiger une preuve rigoureuse, étant donné que les renseignements ne seront pas transmis à ce moment-là aux organismes chargés de l'application de la loi. De la même façon, le second juge à qui il est demandé d'ordonner la production effective des renseignements peut tenir pour acquis que la justification de toute l'atteinte a déjà été établie devant le premier juge.

5. Il est possible qu'une ordonnance de conservation puisse être signifiée et vise le contenu du message plutôt que les données sur le trafic. Les organismes chargés de l'application de la loi pourraient ensuite accéder au message conservé par le FSI grâce à un mandat de perquisition, lequel est beaucoup plus facile à obtenir qu'une ordonnance d'interception.

6. L'ordonnance qui exige la conservation de données stockées chez un FSI pose des risques supplémentaires en ce qui concerne le respect de la vie privée, notamment en ce qui a trait à la sécurité des données au niveau du FSI de même qu'au risque d'un accès illégal notamment de la part de pirates informatiques.

7. On ne doit pas adopter de dispositions qui obligeraient les FSI à stocker toutes les données relatives au trafic et tous les messages pendant un laps de temps donné aux fins d'une action policière hypothétique. De telles dispositions auraient une portée excessive et pourraient sérieusement porter atteinte au droit à la vie privée ainsi qu'à la santé commerciale des FSI canadiens. En effet, les Canadiens pourraient se tourner vers des FSI situés à l'extérieur du Canada pour préserver leur vie privée et ainsi causer des torts considérables à une industrie qui est à la base du commerce électronique canadien.

8. Le principe des ordonnances de conservation des données ne présente pas de problème, mais la portée des articles 16 et 17 de la *Convention sur la cybercriminalité*[35] en soulève certainement un et les délais proposés de 90, 120 ou 180 jours sont trop longs.

9. Les ordonnances de conservation ne devraient s'appliquer qu'aux données informatiques stockées dans les ordinateurs (et non aux documents papier). Elles ne devraient servir qu'à faciliter le déroulement d'une enquête en cours sur une possible contravention aux lois criminelles.

10. Conformément à l'article 487.11 du *Code criminel*, les organismes chargés de l'application de la loi ne devraient pouvoir obtenir une ordonnance de conservation que lorsque l'urgence de la situation rend difficilement réalisable l'obtention d'une ordonnance judiciaire.

11. Si les FSI étaient tenus d'assurer le suivi de toutes les activités en ligne de leurs abonnés, afin que cette information puisse éventuellement servir de preuve devant les tribunaux, il leur faudrait consentir des investissements massifs pour se doter des capacités de stockage requises. Ils pourraient alors devoir augmenter considérablement leurs tarifs, ce qui nuirait au développement des services en ligne au Canada. L'industrie pourrait également être obligée de procéder à des consolidations, ce qui aurait des impacts négatifs pour le droit à la vie privée et la liberté de parole.

12. Cette concentration massive de données sera peu utile pour les organismes d'application de la loi à moins qu'ils ne disposent des ressources nécessaires pour examiner et analyser la très grande quantité de données qui seraient recueillies chaque jour.

D. ORDONNANCES GENERALES DE PRODUCTION

1. Le document de consultation ne justifie pas le recours aux ordonnances de production. Leur nécessité n'a pas été démontrée. On propose toutefois une ordonnance générale de production, qui ressemble à un mandat de perquisition mais qui ne nécessite pas la présence d'un agent de la paix.

2. On ne devrait pouvoir obtenir une ordonnance générale de production qu'en s'adressant à une autorité judiciaire qui applique les normes en vigueur. On ne sait toutefois pas avec certitude pourquoi il serait nécessaire de prévoir des pouvoirs pour forcer les fournisseurs de services à communiquer ces renseignements alors que les organismes chargés de l'application de la loi ont jusqu'ici toujours été en mesure de les obtenir.

E. ORDONNANCES SPECIFIQUES DE PRODUCTION

1. Il y a lieu de s'interroger sur l'hypothèse du document de consultation suivant laquelle les données sur le trafic impliquent nécessairement des attentes moins élevées en matière de respect de la vie privée. Dans le cas de la téléphonie avec fil conventionnelle, les données sur le trafic se limitent en règle générale aux numéros de téléphone composés par un abonné et aux numéros de téléphone des autres personnes qui ont appelé cet abonné. Toutefois, dans le cas des courriels ou des communications par Internet, ces données peuvent comporter une foule de renseignements intimes sur la vie privée des Canadiens.

---

[35] Article 16 – Conservation rapide de données informatiques stockées.
Article 17 – Conservation et divulgation rapides de données relatives au trafic.

F. ORDONNANCES SPECIFIQUES DE PRODUCTION DE DONNEES SUR LE NAA ET L'IFSL

1. Les auteurs du document de consultation suggèrent la création d'une base de données nationale contenant le nom et l'adresse de l'abonné (NAA) client et des renseignements au sujet de l'identité du fournisseur de services locaux (IFSL) pour tous les abonnés canadiens, parce qu'il est difficile pour les organismes d'application de la loi et de sécurité nationale de repérer le fournisseur de services locaux associé à un numéro de téléphone ou à un abonné déterminé.

2. Si la mise sur pied de cette base de données suppose qu'ils doivent entreprendre certaines des démarches pour obtenir des renseignements NAA/IFSL, les organismes chargés de l'application de la loi y penseront à deux fois avant de tenter de les obtenir. De plus, lorsqu'il est associé au nom et à l'adresse d'une personne, un identificateur unique comme un numéro de téléphone vaut la peine d'être protégé en vertu du principe du respect de la vie privée. Il n'est nullement nécessaire de changer les lois et les pratiques actuelles en ce qui a trait à l'accès à ce type de renseignements.

3. On ne devrait pas non plus créer de base de données contenant un registre centralisé des abonnés d'Internet. Autrement, on permettrait aux organismes chargés de l'application de la loi de retracer systématiquement les abonnés inscrits au moyen de leur adresse IP au lieu de s'adresser directement au FSI pour obtenir ces renseignements. Si l'on y donne suite, cette proposition aurait pour effet d'anéantir toute attente en matière de respect de la vie privée et tout anonymat sur Internet.

4. Bien des gens ont plusieurs abonnements de courrier électronique, à la maison et au travail. Il n'est pas inhabituel qu'ils annulent leur abonnement chez un fournisseur pour en souscrire un autre chez un FSI concurrent qui leur offre un meilleur prix ou un meilleur service. La création et le maintien d'une base de données pancanadienne qui soit complète et à jour semble présenter des problèmes de logistique insurmontables, sans compter que les ressources requises serviraient des fins plus utiles ailleurs.

5. Outre le fait que l'on estime que la création d'une telle base de données forcerait davantage le secteur privé à faire de la surveillance, il y a lieu de signaler que l'on craint la prolifération des bases de données gouvernementales renfermant des renseignements au sujet des Canadiens.

6. Cette proposition ne devrait pas être adoptée pour le moment, étant donné que sa nécessité n'a pas été clairement démontrée en établissant que les moyens présentement utilisés pour recueillir des renseignements au sujet des abonnés sont insuffisants ou qu'une telle base de données serait vraiment efficace et que les criminels ne la déjoueraient pas.

7. Dans le document de consultation, il est suggéré aussi que tous les fournisseurs de services soient forcés par la loi de recueillir, vérifier et conserver des renseignements au sujet de l'identité et de l'adresse de tous leurs abonnés. Cette obligation s'étendrait à ceux qui vendent des téléphones cellulaires ou des cartes d'appel prépayées : ils seraient tenus de recueillir (et de communiquer au FSI) des renseignements confidentiels sur l'acheteur, comme son numéro de permis de conduire ou de carte de crédit, ce qui constituerait une grossière ingérence dans la vie privée de ce dernier.

G. INTERCEPTION DU COURRIER ELECTRONIQUE

1. Les questions suivantes auraient dû être posées directement aux Canadiens durant le processus de consultation :

- Un client devrait-il pouvoir légalement souscrire un abonnement de courrier électronique au Canada sans fournir des renseignements personnels de base pour chaque adresse de courriel ?

- Quels types de renseignements personnels les FSI canadiens devraient-il recueillir ?

- Quel degré d'anonymat en ligne devrait-on permettre en vertu de la nouvelle législation ?

- La réexpédition anonyme de courriels au Canada devrait-elle demeurer légale ?

- Le courriel crypté devrait-il être permis à l'intérieur des frontières du Canada, et si oui, à quelles conditions ?

2. Un courriel, qui peut contenir du texte, des sons et des graphiques, constitue une riche source de renseignements intimes au sujet de l'expéditeur, et possiblement aussi au sujet du destinataire. Les tribunaux albertains ont confirmé que le destinataire d'un message électronique, en raison de la *Charte*, pouvait raisonnablement s'attendre à ce que soit respectée la confidentialité de cette communication[36]. Les règles actuelles touchant l'interception des communications privées devraient s'appliquer à l'interception du courrier électronique. L'arrêt Weir ne précise pas à quel degré est diminuée l'attente de vie privée dans le cas de l'entête d'un courriel.

H. AUTRES SUJETS ABORDES PAR LES PERSONNES INTERROGEES

1. Le document de consultation n'indique nulle part que des mesures de reddition de compte sont envisagées.

2. Les propositions contenues dans le document de consultation demandent aux Canadiens d'avoir un niveau élevé de confiance à l'égard des organismes d'application de la loi et du renseignement sans offrir en contrepartie la preuve que ce type de changement à la loi est nécessaire.

3. Il y aurait lieu de prévoir de solides mécanismes de contrôle judiciaire ou autres dans la nouvelle loi sur l'accès légal afin de garantir la transparence, la reddition de compte et l'examen public.

4. Il faudrait créer un organisme de surveillance pour accroître la confiance du public. Il devrait obliger les organismes d'application de la loi à régulièrement produire des rapports sur les mesures d'accès légal qu'ils ont prises ainsi qu'une évaluation de l'efficacité de ces mesures.

5. Un contrôle indépendant de la nature et de la fréquence d'utilisation de tout nouveau pouvoir en matière d'accès légal est essentiel, bien que les intérêts en matière d'application de la loi doivent aussi être protégés. Le recours au Comité de surveillance des activités de renseignement de sécurité du Parlement devrait être envisagé en ce qui concerne tout nouvel accès légal au courrier électronique et aux autres données de communications électroniques.

[36] *R. v. Weir*, [2001] A.J 869 (C.A. Alb.) – cite par un répondant.

CHAPITRE 6 : COMMENTAIRES DES GROUPES DE LA SOCIETE CIVILE

NOMBRE TOTAL DE MEMOIRES REÇUS : 14

Le nombre d'astérisques attribués à chaque commentaire indique la fréquence avec laquelle les répondants ont exprimé cette opinion ou une opinion semblable. Cinq astérisques signifient « très souvent ». Un astérisque signifie généralement qu'une seule réponse a porté sur le sujet, mais cette réponse peut avoir été fournie au nom d'une association ou d'un groupe représentant plusieurs personnes ou organisations. On trouvera la liste des participants à l'annexe D.

A. GENERALITES

1. Le document de consultation n'explique pas clairement les propositions du gouvernement du Canada. Il s'ensuit que les commentaires des groupes de la société civile sont tout aussi vagues. Les participants seront heureux de répondre à toute proposition législative qui pourrait être soumise à l'examen d'un comité parlementaire. *****

2. Le document n'explique pas non plus de manière convaincante comment les propositions contribueraient à lutter efficacement contre le crime organisé ou le terrorisme. Le gouvernement aura sans doute un accès plus grand à la vie privée des Canadiens, mais les criminels et les terroristes dangereux ne seront vraisemblablement pas imprudents au point de se voir assujettir aux mesures proposées. *****

3. Le manque de clarté au sujet du niveau de preuve, de la surveillance et des garanties rend impossible la formulation d'une opinion sur cette proposition. ****

4. Le bien-fondé des propositions formulées par le gouvernement en vue d'élargir l'accès légal aux communications privées n'a pas été démontré, selon les critères posés tant par la Cour suprême[37] que par le Commissaire à la protection de la vie privée du Canada[38]. ****

5. Si des éléments d'information justifient les mesures proposées, il faut les rendre publics pour que l'on puisse vérifier si les avantages sur le plan de la sécurité l'emportent sur les inconvénients liés à une atteinte à la vie privée. En l'absence de tels éléments, les mesures doivent être abandonnées. *****

6. La cybercriminalité, que le problème soit effectif, imminent ou fictif, est invoquée pour justifier un projet de loi qui risque fort de brimer le droit des personnes au respect de leur vie privée. Le Canada ne devrait pas ratifier la *Convention sur la cybercriminalité* si cette mesure est susceptible d'aller à l'encontre des valeurs et des droits garantis par la *Charte des droits et libertés* et interprétés par la Cour suprême du Canada. ****

7. Les propositions établiraient une norme moins exigeante pour l'interception légale, les perquisitions et les saisies de communications en ligne que pour les communications téléphoniques ou postales, par exemple. Aucune justification n'a été donnée pour expliquer cette approche. Les normes prévues dans le *Code criminel* devraient être les mêmes quelle que soit la technologie utilisée.****

8. Le projet de législation et les règlements qui l'accompagnent doivent être rendus publics pour que les citoyens puissent bien les examiner et que les parties intéressées aient suffisamment de temps pour en évaluer l'impact et soumettre leurs commentaires.***

9. Le gouvernement du Canada précise, dans le document de consultation, que les propositions sur l'accès légal visent à « maintenir une capacité adéquate d'accès légal pour les organismes canadiens d'application de la loi et de sécurité nationale dans le contexte de nouvelles technologies ». Or, les propositions *augmenteraient* considérablement la

[37] *R c. Oakes* [1986] 1 R.C.S. 103 - citée par un répondant.
[38] Commentaires sur le *Document de consultation sur l'accès légal*, 25 novembre 2002 - cités par un répondant

capacité technique des organismes en question d'intercepter, de perquisitionner et de saisir les communications électroniques des particuliers, de même que des renseignements personnels sous forme électronique.***

10. Le processus de consultation vise à recueillir les réponses utiles des intervenants et à se servir de ces réponses pour élaborer de meilleures lois. Le succès de ce processus dépend de la volonté du gouvernement de faire connaître franchement et ouvertement ses intentions. Or, il semble que le processus de consultation sur l'accès légal ne se soit pas déroulé de cette manière.***

11. Il y a lieu de rejeter l'idée de « maintenir une capacité adéquate d'accès légal » pour les organismes canadiens d'application de la loi et de sécurité nationale dans le contexte des nouvelles technologies. Non seulement les propositions auraient-elles pour effet d'augmenter cette capacité au-delà de sa portée actuelle, mais encore l'article premier de la *Charte* exige-t-il de justifier selon les principes d'une « société libre et démocratique » toute restriction à un droit garanti. Or, la nécessité d'une telle mesure n'a pas été démontrée de façon empirique dans le cas qui nous occupe.***

12. Les groupes de la société civile aimeraient qu'on leur cite des statistiques qui justifient le besoin d'adopter les changements proposés. Les arguments en faveur de l'attribution des nouveaux pouvoirs proposés ne sont pas suffisamment étayés.***

13. La large définition de base du « fournisseur de services », qui inclut les universités, les collèges et les bibliothèques qui fournissent des services Internet au public, suscite des inquiétudes.***

14. L'Internet est peut-être relativement nouveau, mais les valeurs fondamentales de protection de la vie privée et des libertés publiques sont toujours les mêmes. C'est au prix des sacrifices consentis par les générations qui nous ont précédés, souvent face à des menaces bien plus grandes que celles qui existent aujourd'hui, que nous avons acquis et conservé nos droits. L'héritage laissé par les générations passées fait qu'il est impensable de renoncer à ces droits maintenant, que ce soit sous le prétexte de lutter contre le terrorisme ou encore de s'inspirer d'une mauvaise loi européenne ou américaine.***

15. Les obligations qu'impose la *Convention* en matière d'accès légal vont plus loin que celles qui sont proposées dans le document de consultation. Parmi ces obligations, mentionnons la divulgation des clés de chiffrement et la création de nouvelles infractions criminelles en matière de pornographie juvénile et de surveillance en temps réel de la transmission des données informatiques. Ces obligations devraient toutes faire l'objet de consultations avant que le Canada ne ratifie la *Convention.***

16. Selon notre conception de la vie dans une démocratie, l'État ne devrait pas porter atteinte aux droits, aux libertés ou à la sécurité d'une personne, à moins que ça ne soit clairement justifié. De plus, lorsqu'il existe une preuve convaincante de cette nécessité, la loi ou toute autre mesure proposée par l'État devrait être adaptée de façon à ce que cette atteinte ne soit pas plus importante que nécessaire pour atteindre son objectif.*

17. Tout nouveau texte législatif doit contenir des dispositions spécifiques aux questions relatives au respect de la vie privée chaque fois qu'il y a un risque d'atteinte à la vie privée d'une personne– une référence d'ordre général à la *Charte* et à la *Loi sur la protection des renseignements personnels et les documents électroniques* est insuffisante. *

18. En plus d'être un réseau de communication personnelle, l'Internet est un lieu de rencontre largement utilisé pour échanger des opinions sur la politique, la religion et la culture. Les propositions menacent donc non seulement le droit à la vie privée des Canadiens qui est protégé par l'article 8 de la *Charte*, mais aussi la liberté d'expression et la liberté d'association protégées par l'article 2 et le droit à la liberté de sa personne garanti par l'article 7. *

19. Selon les données de différents organismes américains d'application de la loi, ce sont des obstacles technologiques et administratifs, plutôt que juridiques, qui expliquent la plupart des difficultés éprouvées dans les enquêtes et les poursuites en matière de cybercriminalité. Ces difficultés concernent notamment les registres insuffisants tenus par les FSC, l'incapacité de procéder à la conservation des données à l'étranger, l'incapacité de déchiffrer les messages codés et l'absence de protocoles uniformes en matière de partage de données. *

20. Si les organismes d'application de la loi éprouvent des difficultés avec les nouvelles technologies de communications, la solution n'est pas d'abaisser les normes juridiques en matière d'interception, mais plutôt de leur fournir l'expertise technique et l'équipement dont ils ont besoin pour fonctionner dans l'environnement en évolution. *

21. La protection de la confidentialité des communications électroniques devrait être *plus forte* que celle qui est accordée aux communications non électroniques, compte tenu des possibilités sans précédent qui sont offertes aux organismes d'application de la loi de faire de la surveillance et de porter atteinte au droit à la vie privée. *

22. Les demandes d'autorisation et les interceptions effectivement réalisées au Canada ont diminué au cours des vingt dernières années[39]. Aucune explication n'a été avancée pour justifier cette baisse et aucune donnée statistique n'a été citée au sujet de la fréquence des autorisations d'interception ou sur le nombre d'entre elles qui ont été abandonnées pour cause de capacités techniques insuffisantes. *

23. Le fait qu'une loi proposée puisse être avantageuse pour les organismes d'application de la loi ne met pas fin au débat sur la question de savoir si cette loi est constitutionnelle ou si elle est autrement souhaitable. Il s'agit plutôt d'un point de départ pour la discussion. *

24. Tout nouveau pouvoir doit faire l'objet d'un contrôle. On devrait élaborer un mécanisme unique de contrôle prévoyant des règles strictes et une supervision judiciaire. Il faut éviter la multiplication des mécanismes. *

25. La tension entre le droit à la vie privée et la sécurité n'est pas une situation où les différents éléments s'annulent. Il faut éviter d'accorder trop de poids à ceux qui prétendent qu'on doit à tout prix conférer des pouvoirs accrus aux organismes chargés de l'application de la loi. Un législateur souple cherchera à proposer des solutions innovatrices qui tiennent compte à la fois de l'importance de la sécurité et de celle du respect de la vie privée. Ce n'est qu'en surveillant de près les mesures prises par les organismes chargés de l'application de la loi que le Canada continuera à incarner les idéaux consacrés par sa *Charte*. *

B. OBLIGATIONS DE GARANTIR LA CAPACITE D'INTERCEPTION

1. Le gouvernement n'a pas démontré la nécessité de cette infrastructure de surveillance massive. Par exemple, on ne connaît pas le nombre exact d'enquêtes dont le déroulement a été sérieusement entravé en raison de l'insuffisance des capacités techniques. ****

2. Il n'est pas nécessaire d'accroître les pouvoirs pour favoriser l'interception de communications sur le réseau Internet au Canada. Les lois actuelles prévoient des pouvoirs amplement suffisants pour faire enquête sur les utilisations criminelles d'Internet lorsque la police est en mesure de convaincre un juge qu'il existe des motifs raisonnables d'ouvrir une enquête. ***

3. Si les capacités d'interception proposées ne sont requises qu'en cas de « amélioration significative de leurs systèmes ou de leurs réseaux », les FSI hésiteront peut-être à améliorer leurs activités ou leurs capacités, ce qui pourrait restreindre l'instauration de nouveaux services ou de services améliorés et pourrait entrer en conflit avec la politique canadienne de télécommunications[40]. ***

4. La plupart des difficultés auxquelles sont confrontés les organismes d'application de la loi et de sécurité nationale, en ce qui concerne l'accès aux moyens modernes de télécommunications, seraient mieux résolues par les techniciens de Silicon Valley que par le législateur, le Congrès ou Bruxelles. **

[39] Intervention du ministère de la Justice lors de la table ronde sur l'accès légal organisée à Ottawa le 21 octobre 2002- cité par un répondant.

[40] Alinéa 7g) –*Loi sur les télécommunications*, Lois du Canada, chapitre 38. Cité par un répondant.

5. Le Canada devrait prendre la peine de vérifier en quoi la transmission de données diffère du service téléphonique traditionnel[41] et comment les organismes chargés de l'application de la loi devraient tenir compte de ces différences. Cet aspect a causé de sérieuses difficultés aux États-Unis et aux Pays-Bas lors de la rédaction des dispositions législatives sur l'accès légal. **

6. Si le tribunal autorise la police à surveiller des communications privées, l'effet de cette autorisation ne doit pas être annulé par l'absence de moyens techniques. *

7. En plus de présumer la neutralité des moyens de communications[42], alors qu'aucun motif n'a été démontré pour justifier cette façon de faire, le gouvernement passe sous silence, dans le document de consultation, un corollaire important, en l'occurrence le principe de la neutralité technologique[43]. *

8. Pour que les données interceptées soient utiles, il est nécessaire que les organismes chargés de l'application de la loi en comprennent le contenu. Les grands criminels peuvent leur rendre la tâche plus difficile en recourant à du cryptage facile à obtenir. Il s'ensuit que les criminels, les terroristes et d'autres minorités qui recourent au cryptage pour toutes les communications sur réseau seront les seuls à bénéficier d'une protection en ligne de leur vie privée. *

9. Les fournisseurs de services du secteur privé sont-ils des représentants de l'État ? Les renseignements recueillis par les FSP sont-ils sujets aux dispositions de la *Charte* relatives aux fouilles, aux perquisitions et aux saisies abusives ? Aucune de ces questions n'est abordée dans le document de consultation. *

C. EXEMPTION

1. Les circonstances justifiant une ordonnance d'exemption devraient être précisées, ainsi que les critères permettant de déterminer quand et pendant combien de temps ces ordonnances seront valides. Toute règle concernant le pouvoir d'exemption doit être claire et transparente. *

2. Les obligations en matière d'accès légal sont particulièrement exigeantes pour les petits FSI et pour les organismes sans but lucratif qui fournissent des services Internet à leurs membres. Les exemptions proposées n'ont rien pour rassurer les intéressés, puisqu'elles risquent d'être supprimées plus tard. *

D. COUTS

1. Les propositions exigent des Canadiens ou de leurs fournisseurs de services de communication qu'ils paient pour la surveillance, ce qui est incorrect en principe et impraticable dans les faits. *

2. Le gouvernement fédéral devrait accorder un appui financier aux FSI canadiens qui ont besoin d'installations techniques supplémentaires pour répondre à leur obligation d'assurer la capacité de conservation des données. *

3. Les coûts accrus entraînés par la fourniture de cette capacité d'interception et d'appui auraient des conséquences sérieuses sur les fournisseurs de services régionaux Libertel qui comptent sur le travail des bénévoles et sur les dons pour poursuivre leurs activités. *

E. ORDONNANCES GENERALES DE PRODUCTION

1. Les FSI ont pour tâche de fournir des services à leurs clients. Cette tâche ne doit pas consister également à les surveiller au nom de l'État. On ne doit pas se servir d'ordonnances de production dans le but de se soustraire aux

[41] Ou service téléphonique de base.
[42] Tous les moyens de communications (avec fil, courrier électronique, communications sans fil, etc.) bénéficient du même traitement en vertu de la loi. Définition fournie par un répondant.
[43] La neutralité technologique est une façon de rédiger les lois et les règlements sans faire mention d'une technologie déterminée et ce, dans le but de limiter la nécessité de réviser par la suite le texte pour tenir compte de l'évolution de la technologie. Définition fournie par un répondant.

critères exigeants qu'il faudrait respecter si les organismes d'application de la loi procédaient eux-mêmes à la perquisition ou à l'interception. ***

2. Le *Code criminel* devrait être modifié par l'insertion d'une disposition permettant le prononcé d'ordonnances générales de production. Cette ordonnance ne devrait cependant être utilisée que pour faciliter l'accès à l'information provenant des FSC. *

3. Certains s'opposent à la création d'une ordonnance générale de production si l'on n'oblige pas la personne qui la réclame à présenter des éléments de preuve convaincants pour démontrer que les pouvoirs prévus par les mandats sont insuffisants. Si les ordonnances générales de production sont néanmoins créées, elles devraient être assujetties aux mêmes garanties procédurales que les mandats de perquisition (ou d'interception, le cas échéant). *

4. À toutes fins utiles, les ordonnances de production sont des mandats et elles doivent être assujetties à toutes les exigences et protections prévues par la partie XV du *Code criminel* et par la jurisprudence. Le gouvernement fédéral n'a pas fourni d'éléments d'information pour démontrer pourquoi l'élargissement de ces pouvoirs était nécessaire ou pourquoi le mandat de perquisition actuel combiné à une ordonnance d'assistance ne suffisait pas. *

5. Dans le même ordre d'idées, il est difficile de voir comment les ordonnances anticipatoires commanderaient l'application d'une norme différente que celle qui est présentement utilisée pour les fouilles, les perquisitions et les saisies ou encore pour l'interception des communications. *

6. Comme les organismes chargés de l'application de la loi ne disposent d'aucun autre moyen pour obtenir ce genre d'informations électroniques et qu'en cas d'urgence, les tribunaux peuvent leur faciliter la tâche en prononçant une ordonnance, il semble inutile d'examiner plus à fond les changements proposés. *

7. Toute interception et / ou perquisition et saisie de communications électroniques devrait nécessiter l'approbation du tribunal, indiquer la personne précise qui est visée ainsi que les renseignements à intercepter et à saisir et exposer les motifs justifiant l'interception ou la saisie. Toutes les ordonnances devraient prévoir des délais d'exécution précis. *

8. Si elles sont adoptées, les ordonnances générales de production devraient contenir des modalités pour garantir la confidentialité et la sécurité des renseignements recueillis qui sont destinés à être produits. *

9. Les dispositions législatives actuelles en matière de fouilles, de perquisitions et de saisies exigent que l'intéressé soit avisé après coup. Toute ordonnance de production devrait contenir la même exigence. *

10. L'ordonnance générale de production ne devrait pas être une ordonnance autonome et ne devrait être rendue que si un mandat de perquisition ou une autorisation d'interception a déjà été approuvé. *

11. Le recours systématique aux services de communications perfectionnés par le public a créé la perception que ces communications sont privées et qu'elles ne peuvent faire l'objet d'un examen de la part des organismes chargés de l'application de la loi que si des motifs raisonnables sont invoqués. Les tribunaux devraient être les arbitres ultimes en ce qui concerne la norme de preuve requise en matière de protection de la vie privée des personnes. *

12. Un mandat de perquisition délivré au Canada ne peut être exécuté à l'extérieur du Canada pour obtenir des documents qui se trouvent à l'étranger. Il faut utiliser des procédures d'entraide juridique pour obtenir des documents qui se trouvent à l'étranger. Le recours aux ordonnances de production permettrait de contourner efficacement cette procédure et de neutraliser les garanties qu'elle accorde tant aux personnes se trouvant en sol canadien qu'à celles qui sont à l'étranger. *

13. Il ne devrait pas être possible d'obtenir une ordonnance de production pour obliger des suspects à participer à une enquête dirigée contre eux par la production de documents. Une telle ordonnance irait très probablement à l'encontre des garanties de la *Charte* contre l'auto-incrimination. *

F. ORDONNANCES SPECIFIQUES DE PRODUCTION DE DONNEES SUR LE TRAFIC

1. Nous prions instamment le gouvernement de rejeter toute mesure législative qui permettrait aux organismes chargés de l'application de la loi d'obtenir des données sur le trafic selon une norme moins exigeante. Dans cette proposition, le gouvernement dépeint les données sur le trafic comme des informations ayant peu de valeur en ce qui concerne le respect de la vie privée, en faisant valoir qu'elles devraient être assujetties à la même norme moins élevée que celle qui s'applique aux enregistreurs de numéros de téléphone (ENT). Or, les données sur le trafic en révèlent bien plus sur les activités d'une personne que celles qui sont consignées par les ENT. **

2. Comme il semble que les outils d'enquête dont disposent les organismes chargés de l'application de la loi ne permettent pas de séparer de façon fiable le contenu des données sur le trafic, les deux types de données devraient bénéficier du même degré de protection constitutionnelle. **

3. Si le droit à la vie privée de l'individu doit être protégé, nous ne pouvons nous permettre d'attendre que ce droit ait été violé pour le revendiquer. Ce principe est inhérent à la notion de protection contre les fouilles, les perquisitions et les saisies abusives[44]. **

4. Au lieu de créer une ordonnance spécifique de production à cette fin, le législateur devrait modifier les dispositions actuelles que l'on trouve à l'article 492.2 du *Code criminel* au sujet des renseignements téléphoniques. Les données sur le trafic devraient se limiter aux adresses Internet, aux adresses de courrier électronique et aux informations sur le routage. *

5. Les tribunaux ont jugé que la cueillette de données ENT sans approbation judiciaire contrevenait à la partie VI du *Code criminel*, ce qui montre que les ENT se situent dans une zone grise et que les ordonnances de cueillette de données sur le trafic devraient toujours se faire sous la surveillance du tribunal. *

G. ORDONNANCES SPECIFIQUES DE PRODUCTION DE RENSEIGNEMENTS SUR LE NOM ET L'ADRESSE DE L'ABONNE (NAA) ET SUR L'IDENTITE DU FOURNISSEUR DE SERVICES LOCAUX (IFSL)

1. La création d'une base de données nationale renfermant des renseignements personnels - même s'ils se limitent aux données sur les abonnés - risque de donner lieu à des abus et devrait donc être évitée. Elle revient à permettre à l'État de recueillir des renseignements personnels avant la perpétration réelle ou appréhendée d'une infraction. ****.

2. Le gouvernement ne démontre pas de façon satisfaisante, dans le document de consultation, les difficultés urgentes auxquelles sont confrontés les organismes chargés de l'application de la loi, qui justifieraient soit le prononcé d'une ordonnance spécifique de production de renseignements NAA/IFSL ou la mise sur pied d'une base de données nationale contenant des renseignements sur les abonnés. ***

3. Le critère suivant posé par le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) au sujet de la divulgation de l'IFSL par Bell Canada est approprié et devrait être étendu aux autres fournisseurs de services canadiens[45] :

> Pour obtenir l'information, un organisme chargé de l'application de la loi doit démontrer qu'il en a l'autorisation et indiquer, selon le cas :
>
> - qu'il a des motifs raisonnables de croire que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales ;
>
> - que la communication est demandée aux fins du contrôle d'application du droit canadien, provincial ou étranger, de la tenue d'enquêtes liées à ce contrôle d'application ou de la collecte de renseignements en matière de sécurité en vue de ce contrôle d'application ;

[44] *R. c. Dyment* [1988] 2 R.C.S. 417, note 1, au par. 23, cité par plusieurs personnes répondants.
[45] Décision télécom du CRTC 2002-12, le 12 avril 2002, par. 22é

- qu'elle est faite en raison d'une situation d'urgence menaçant la vie, la santé ou la sécurité de toute personne, ou afin de permettre à un organisme chargé de l'application de la loi de remplir ses obligations afin d'assurer la protection et la sécurité des personnes et de la propriété. ***

4. Ce n'est pas parce qu'on peut obtenir des renseignements sur le NAA simplement en consultant un répertoire que l'on devrait pour autant accorder aux organismes chargés de l'application de la loi un accès illimité aux renseignements sur le NAA en ce qui concerne les abonnés qui choisissent de protéger leur vie privée. Ces personnes ont à tout le moins des attentes élevées en ce qui concerne le respect de leur vie privée. ***

5. Les renseignements sur les adresses Internet ne devraient certainement pas faire l'objet d'une norme d'accès moins élevée, compte tenu du fait que la possibilité d'établir un lien entre ces renseignements et des individus déterminés permettrait la cueillette d'une quantité considérable de renseignements personnels. ***

6. Les FSC ne devraient pas être obligés de recueillir des renseignements sur leurs abonnés qu'ils ne recueillent pas déjà dans le cadre normal de leurs activités commerciales. L'obligation proposée aurait probablement des incidences sur la plupart des fournisseurs de services et des détaillants qui vendent des cartes d'appel prépayées et d'autres cartes d'appels ou téléphones anonymes. Ainsi que le Commissaire à la protection de la vie privée du Canada l'a signalé[46], une telle mesure constituerait une grossière ingérence dans la vie privée des abonnés en plus de favoriser le détournement ou la perte de données (et les menaces qui pourraient en découler, telles que l'usurpation d'identité). ***

7. Les organismes d'application de la loi et de sécurité nationale devraient être obligés de demander l'autorisation du tribunal pour pouvoir obtenir des renseignements au sujet d'un abonné ou de son fournisseur de services lorsqu'ils mènent une enquête sur cette personne. **

8. Nous ne devrions pas imposer une charge plus lourde ou accorder une protection moindre aux fournisseurs de services, aux détaillants et aux utilisateurs finaux simplement parce qu'ils souhaitent se prévaloir des solutions qu'offre la technologie comme alternative à Postes Canada. *

9. Les bases nationales de données créent un seul point de vulnérabilité pour ceux qui sont intéressés à un accès non autorisé à des renseignements personnels précieux. Une base de données de ce genre constituerait par ailleurs une violation flagrante de la *Loi sur la protection des renseignements personnels*, notamment de ses articles 4, 5 et 7[47]. *

H. ORDONNANCE DE CONSERVATION DE DONNEES

1. Les ordonnances de conservation n'existent pas encore en droit canadien. À l'exception des dispositions de la *Convention sur la cybercriminalité*, rien n'a été invoqué pour justifier la création de cette nouvelle ordonnance, qui équivaut à une forme limitée de stockage des données. La proposition visant à créer ce type d'ordonnance ne devrait pas être adoptée sans justification évidente. *****

2. Cette ordonnance, telle qu'adoptée dans d'autres pays (notamment au Royaume-Uni) constitue une étape risquant de mener au mécanisme permettant le stockage des données à long terme. Elle pourrait être utilisée comme un « moyen détourné » d'obtenir du tribunal une autorisation d'accès et de se soustraire aux critères plus exigeants qui s'appliquent aux mandats ordinaires. En tout état de cause, cette ordonnance représenterait davantage un élargissement qu'un maintien des capacités actuelles en matière d'accès légal et elle devrait être rejetée pour cette seule raison. ***

3. Si jamais elles sont adoptées en droit canadien, les ordonnances de conservation devraient être assorties de délais précis, exiger le respect de la confidentialité et de la sécurité des renseignements visés et interdire la divulgation des données tant qu'une ordonnance de production n'aura pas été obtenue d'un juge ou d'un tribunal. ***

[46] Commentaires sur le *Document de consultation sur l'accès légal*, 25 novembre 2002 – cité par un répondant.
[47] L.R.C. (1985), ch. P-21- citée par un répondant.

I. PROPAGATION DE VIRUS INFORMATIQUES

1. Les activités légitimes des particuliers et des compagnies qui possèdent des virus pour se livrer à de la recherche analytique, à de la conception ou à l'enseignement ou pour détecter et neutraliser les virus ne devraient pas être interdites. De même, on ne devrait pas déclarer coupable d'une infraction la personne dont l'ordinateur est à son insu infecté d'un virus non détecté ou d'un autre dispositif semblable. **

2. L'interdiction envisagée par le gouvernement visant les virus recueille de larges appuis. Il faut cependant faire la distinction entre un virus ordinaire et un virus latent ou non activé. *

J. INTERCEPTION DU COURRIER ELECTRONIQUE

1. Le courrier électronique devrait recevoir le même traitement que le courrier de première classe de la part du gouvernement canadien qui devrait lui reconnaître la même protection que toute autre communication privée. Ainsi, les règles de preuve prévues par la loi et par la common law s'appliqueraient de la même façon au courrier électronique qu'au courrier postal. *****

2. Le *Code criminel* devrait être modifié pour bien préciser que le courrier électronique, du moins lorsqu'il est en train d'être transmis, constitue une « communication privée » au sens de l'article 183. Il ferait alors l'objet des mêmes garanties procédurales que toutes les autres communications interceptées en vertu de cette disposition. ***

3. Le *Code criminel* devrait préciser dans quels cas un message électronique cesse d'être une communication susceptible d'être interceptée et quand il devient un document pouvant faire l'objet d'une perquisition et d'une saisie[48]. **

4. Les Canadiens ont, lorsqu'ils utilisent le courrier électronique, des attentes en matière de protection de leur vie privée qui sont semblables à celles qu'ils ont en ce qui concerne les autres formes de communication. Le traitement que la loi réserve au courrier électronique ne devrait pas dépendre des capacités technologiques, mais bien des valeurs de notre société. Si nous souhaitons communiquer de façon privée par courrier électronique, nous devons interpréter nos lois en conséquence. *

5. Les FSI sans but lucratif, exploités par des groupes communautaires qui offrent des listes confidentielles d'adresses de courrier électronique pour permettre à des avocats de consulter des intervenants communautaires au sujet de cas difficiles, des questions relatives à la réforme du droit et à d'autres questions épineuses, craignent que la loi proposée risque de porter atteinte à la vie privée des intervenants et des autres personnes qui utilisent ce service. *

6. Bien qu'ils soient des compagnies privées, les FSI devraient être assujettis à la réglementation de l'État parce qu'ils sont chargés du service essentiel que constitue la livraison du courrier électronique. *

K. AUTRES SUJETS ABORDES PAR LES PERSONNES INTERROGEES

Questions extraterritoriales

1. La collaboration avec d'autres États et la transmission des données interceptées et saisies en vertu des traités d'entraide juridique soulèvent de sérieuses questions de souveraineté, notamment en ce qui concerne les risques de compromettre des droits protégés par la *Charte*. La double incrimination constitue un problème particulier. Le Canada doit protéger ses citoyens selon les règles du droit canadien. *

2. On craint sérieusement que les Canadiens risquent d'être assujettis aux lois de pays étrangers à la suite d'une demande de collaboration émanant d'un autre pays. Les responsables canadiens de l'application de la loi ne devraient

[48] Par exemple, si le message électronique a déjà été envoyé au destinataire, mais qu'il est encore emmagasiné chez le FSI, il est possible que l'accès légal constitue une saisie plutôt qu'une interception.

appliquer que les lois canadiennes et n'ont pas à offrir leur aide pour faciliter l'application de lois étrangères qui offrent des différences importantes. *

CHAPITRE 7 : COMMENTAIRES DU GRAND PUBLIC[49]

NOMBRE TOTAL DE MEMOIRES REÇUS : 219

Lorsque c'était possible, nous avons conservé les expressions utilisées par les membres du public dans leurs réponses afin que le lecteur ait une idée fidèle des commentaires formulés.

Le nombre d'astérisques attribués à chaque commentaire indique la fréquence avec laquelle les répondants ont exprimé cette opinion ou une opinion semblable. Cinq astérisques signifient « très souvent ». Un astérisque signifie généralement qu'une seule réponse a porté sur le sujet.

A. GENERALITES

1. Le grand public est très reconnaissant d'avoir eu l'occasion de formuler des commentaires sur ces propositions. *****

2. On ne sait pas avec certitude si les propositions faciliteraient réellement la lutte contre le crime et le terrorisme. Aucun argument solide n'a été invoqué pour démontrer comment l'accès aux activités en ligne de simples particuliers peut par ailleurs faciliter la réalisation de ces objectifs. ****

3. Les coûts sont élevés, les risques sont élevés et on ne sait pas exactement quel avantage présente les modifications législatives proposées que n'offre pas déjà la législation actuelle. ***

4. Un observateur extérieur pourrait se demander si, dans son document de consultation, le gouvernement cite la *Convention sur la cybercriminalité* comme argument accessoire plutôt qu'en tant que justification solide des propositions soumises. ***

5. Il est fort inquiétant que des traités internationaux comme *la Convention sur la Cybercriminalité* soient signés sans consultation démocratique et présentés ensuite au public comme s'il était essentiel qu'ils soient ratifiés. **

6. Le document de consultation ne réussit pas à démontrer comment l'Internet a crée « des problèmes importants pour les enquêteurs ». Aussi, dans le cas de l'Internet, « la nécessité de disposer d'équipement de pointe » semble se résumer à l'existence de renifleurs de paquets qui sont largement employés par les fournisseurs de service Internet et coûtent quelques milliers de dollars chacun. *

7. Lorsque le Commissaire à la protection de la vie privée du Canada condamne des propositions, celles-ci devraient être retirées sur-le-champ. *

8. Les modifications législatives proposées constituent un exemple de mesure par laquelle le gouvernement dérogerait à la *Charte* « pour protéger la population ». Nous n'avons pas besoin de ce genre de protection. Il vaut mieux vivre dans la peur que de voir nos droits et libertés supprimés par ceux (le gouvernement) qui sont censés les protéger. *

9. On n'établit pas dans le document de consultation de justification à l'effet que les Canadiens méritent moins de protection de leur vie privée lorsqu'ils utilisent des technologies de communication numériques plutôt qu'analogiques, ou en fait lorsqu'ils utilisent des moyens électroniques plutôt qu'un moyen traditionnel. *

10. La vie privée et la sécurité des personnes qui recourent aux communications électroniques est bien davantage compromise par les activités criminelles commises en ligne telles que l'usurpation d'identité, la consultation illicite de

[49] Font partie de ce groupe les personnes qui travaillent pour des sociétés, des universités ou d'autres organisations et qui ont fourni des réponses sans indiquer qu'elles s'exprimaient au nom de leur employeur.

bases de données et les actes irréguliers commis par les fournisseurs de services que par toute autre activité provenant d'une autre source. *

11. La définition du « fournisseur de services » devrait être révisée, de manière à exclure, par exemple, les réseaux domestiques. *

B. OBLIGATION DE GARANTIR LA CAPACITE D'INTERCEPTION

1. Dans le document de consultation, le gouvernement fédéral affirme que les FSI n'ont présentement pas les moyens de permettre aux organismes d'application de la loi de saisir du matériel d'interception. C'est faux. Pratiquement toutes les communications transmises par réseaux peuvent déjà être interceptées avec l'équipement approprié. ***

2. Le cryptage des données est largement employé par les criminels et les terroristes lorsqu'ils communiquent sur des réseaux privés et publics, y compris l'Internet. Les techniques de cryptage sont souvent indétectables, impossibles à intercepter et elles peuvent rendre inefficaces les techniques d'interception utilisées par les organismes d'application de la loi et les fournisseurs de services de communication. ***

3. Le furetage anonyme sur Internet est faisable et est appuyé par le Consortium du World Wide Web (W3C), le groupe de travail IETF (Internet Engineering Task Force), le 3GPP (Third Generation Partnership Project) et d'autres organismes de normalisation. Les dispositifs de banalisation sur Internet peuvent aussi rendre inutilisables les techniques d'interception. ***

4. Si elles sont trop exigeantes, les conditions d'accès imposées aux FSI de premier niveau risquent d'empêcher le développement de petits fournisseurs dans les régions rurales et de forcer les petits FSI à cesser leurs activités. ***

5. Il est très difficile de justifier de pratiquer une brèche en matière de sécurité dans le réseau d'un FSI afin de faciliter l'accès des organismes d'application de la loi. Supposons qu'on assiste à un piratage de données ou à une usurpation d'identité. Qui serait responsable ? Le journal d'exploitation du serveur constitue un moyen amplement suffisant pour retracer les méfaits. **

6. Le fait que l'on s'attende à ce que chaque FSI soit équipé de façon appropriée et qu'il ait la capacité de fournir une série non spécifique de renseignements sur les statistiques, l'interception et leurs journaux d'exploitation constitue une attente beaucoup trop vague et fort probablement trop coûteuse pour pouvoir être mise en œuvre. Il serait plus pratique de demander à chaque FSI de collaborer avec les organismes d'enquête sur les moyens d'établir un lien entre le matériel d'interception, de saisie et d'enregistrement des opérations et le service en question. *

7. On ne devrait adopter aucune loi qui instaure un système officiel de points d'interception des données disséminés un peu partout dans l'infrastructure canadienne des communications. Un tel système se prête à des abus, surtout dans le cas des réseaux à commutation de paquets ou de cellules. *

8. Il est raisonnable de permettre les mêmes capacités d'interception sur Internet ou des capacités similaires à celles qui existent présentement dans le cas du courrier postal et du service téléphonique. Ni plus, ni moins. *

9. Voici quelques solutions pratiques en ce qui concerne les capacités *:

a. s'assurer que tout le courrier électronique sur Internet est intercepté / interceptable par l'État et (au besoin) est enregistré;

b. mettre sur pied un système permettant d'obtenir du tribunal une ordonnance enjoignant à l'intéressé à remettre les clés de cryptage ou à installer des programmes renifleurs;

c. s'assurer que les organismes chargés d'assurer la sécurité de l'État qui interceptent et déchiffrent (ou tentent de déchiffrer) des communications à l'insu de l'expéditeur ou du destinataire font l'objet d'un contrôle rigoureux de la part des tribunaux et qu'ils agissent comme des organismes de surveillance indépendants.

C. EXEMPTION

1. Il est tout à fait inutile de dresser une liste précise des FSCs qui sont soustraits à l'agrément[50]. Les règles de procédure qui régissent les perquisitions et les interceptions légitimes suffisent à ce chapitre. C'est au juge saisi d'une demande d'ordonnance qu'il appartient d'accorder ou non une exception. *

D. COUTS

1. S'il a besoin de l'aide d'un FSC et que cela entraîne pour ce dernier des coûts supérieurs à ses coûts d'exploitation normaux, l'organisme d'application de la loi assume ces coûts supérieurs. Ils ne devraient pas être assumés par le fournisseur de service ni refilés au client. ***

2. Les frais supportés par les organismes qui procèdent à de l'interception et à de la surveillance en ligne et ailleurs sur le réseau devraient soumettre un rapport annuel au Parlement et mettre ce rapport à la disposition du public canadien. *

3. À cause de l'imprévisibilité des enquêtes menées par les organismes d'application de la loi et du fait que ceux-ci sont susceptibles de mener de telles enquêtes au hasard, les coûts et les outils associés aux saisies et à l'interception policières devraient être supportés par l'organisme d'application de la loi et non par le fournisseur de services. *

4. L'indemnité financière équitable à verser aux FSI devrait comprendre les frais de main-d'œuvre directs associés à la collaboration offerte aux organismes d'application de la loi, le manque à gagner découlant de l'impossibilité d'affecter le personnel à d'autres tâches rémunérées, les dépenses d'immobilisations afférentes au matériel informatique, les logiciels, les permis et les frais d'entretien. *

E. ORDONNANCES GENERALES DE PRODUCTION

1. Aucun FSI ne devrait agir comme organisme de collecte de renseignements pour le compte du gouvernement canadien. S'il veut obtenir de l'information, et en a besoin, le gouvernement devrait faire la recherche de données, les recueillir et les stocker. Le FSI doit seulement être tenu de fournir les installations lorsqu'il existe une ordonnance légitime à cet effet. ****

2. Les ordonnances de production sont inutiles, compte tenu de la capacité des organismes chargés de l'application de la loi d'obtenir des renseignements avec les moyens déjà existants. Les raisons invoquées pour justifier les ordonnances préventives sont absurdes. ***

3. Toute tentative de surveillance des communications doit être autorisée par le tribunal. La demande visant à obtenir cette autorisation doit être formulée en des termes explicites et préciser qui, quoi, quand et où elle doit avoir lieu (ainsi que la durée de la période de surveillance). Cette demande ne doit pas être formulée en des termes vagues et l'autorisation demandée ne doit pas excéder la période maximale prévue par la loi. Un délai d'un mois semble raisonnable. ****

4. Il est nécessaire que les ordonnances de production soit explicites et précises. Les recherches futiles devraient être expressément interdites. ***

5. Les organismes chargés de l'application de la loi ne devraient pas être autorisés à surveiller les opérations privées sans que le tribunal n'exerce un contrôle judiciaire par le biais d'une ordonnance préventive. **

[50] L'identification publique des fournisseurs de services exemptés permet aux criminels de repérer les abris sûrs.

F. ORDONNANCES SPECIFIQUES DE PRODUCTION EN MATIERE DE DONNEES RELATIVES AU TRAFIC

1. Il est inacceptable que la police exige des FSI qu'ils tiennent un journal des sites Web visités par chaque abonné au cas où ils souhaiteraient les épier par la suite. Les particuliers ne devraient pas faire l'objet d'une enquête ou être soupçonnés en fonction de leur choix de lectures, que ce soit sur le réseau Internet ou ailleurs. *

2. Les en-têtes de messages électroniques ont tendance à inclure beaucoup plus d'éléments d'information qu'une enveloppe postale. Ils comprennent le plus souvent non seulement le nom du destinataire, mais aussi la source, l'objet et la taille du message. *

G. ORDONNANCES SPECIFIQUES DE PRODUCTION DE RENSEIGNEMENTS SUR LE NOM ET L'ADRESSE DE L'ABONNE (NAA) ET SUR L'IDENTITE DU FOURNISSEUR DE SERVICES LOCAUX (IFSL)

1. Nous n'avons nullement besoin d'une autre base de données pancanadienne de dossiers personnels. Il n'existe pas de répertoire pancanadien des abonnés du téléphone ou des utilisateurs de la poste. Il ne doit donc pas y en avoir pour les utilisateurs d'Internet. Une base de données de ce genre constituerait une accumulation dangereuse. Les bureaucrates peuvent-ils garantir que cette base de données ultra-sensibles sera entièrement à l'abri du piratage informatique ? *****

2. Il n'existe pas de répertoire pancanadien des abonnés du téléphone ou des utilisateurs de la poste. Il ne doit donc pas y en avoir pour les utilisateurs d'Internet. Une telle suggestion est tout à fait inacceptable. ****

3. Une base de données de ce genre constituerait une accumulation dangereuse. Les bureaucrates peuvent-ils garantir que cette base de données ultra-sensibles sera entièrement à l'abri du piratage informatique ? **

4. Dans le document de consultation, il est clair que ce type d'ordonnance est requis pour permettre aux organismes chargés de l'application de la loi de procéder à des « expéditions de pêche » lorsque le prononcé d'une ordonnance judiciaire n'est pas justifié. Il est essentiel que les tribunaux exercent un contrôle en la matière. *

5. Les FSC ne devraient en aucun cas être tenus de recueillir des renseignements qu'ils ne collectent pas normalement dans le cadre de leurs activités quotidiennes. Agir autrement reviendrait à contrevenir aux pratiques commerciales légitimes qui interdisent la cueillette de données. Les fournisseurs de services verraient leurs coûts augmenter et prendraient à leur charge des tâches qui sont normalement assumées par les organismes chargés de l'application de la loi. *

6. Des peines sévères devraient sanctionner l'accès illégal à une base de données d'un FSI dans laquelle sont consignées les activités en ligne d'une personne ainsi que d'autres données personnelles. *

H. ORDONNANCES D'ASSISTANCE

1. Les ordonnances d'assistance devraient faire l'objet d'une demande expresse. Le requérant devrait préciser l'assistance qu'il requiert. *

2. Les grilles tarifaires pour l'assistance offerte aux organismes chargés de l'application de la loi devraient s'inspirer de celles qu'utilise le gouvernement lorsqu'il répond aux demandes émanant du public en vertu de la *Loi d'accès à l'information*. *

I. ORDONNANCE DE CONSERVATION DE DONNEES

1. Les ordonnances de conservation de données devraient s'appliquer à toutes les formes de données indépendamment du moyen de communication. Elles ne devraient pas être valides plus longtemps qu'il n'est raisonnable pour obtenir l'ordonnance de production nécessaire (par exemple, une semaine). ***

2. La conservation proposée des messages électroniques et des autres communications Internet destinés à être utilisées par les organismes chargés de l'application de la loi augmentera nécessairement l'utilisation de logiciels de cryptage par le public. **

J. PROPAGATION DE VIRUS INFORMATIQUES

1. La *Convention* déclare illégal le fait pour des compagnies de logiciels de créer ou de stocker des virus et elle érige en acte criminel le fait pour les chercheurs universitaires et les FSI d'étudier le comportement des virus. Ces propositions sont déraisonnables. *****

2. La question de la criminalisation des logiciels de virus devrait être réexaminée pour inclure tous les types de logiciels nuisibles, c.-à-d. les logiciels (ou dispositifs) mis au point ou possédés *dans le but de porter atteinte* à l'intégrité, la disponibilité ou la confidentialité des systèmes informatiques et des réseaux de télécommunications. ***

3. En vertu des dispositions actuelles du *Code criminel*, seules les conséquences de la propagation d'un virus informatique et les tentatives de propagation constituent des actes criminels. Il est nécessaire de modifier les dispositions actuelles. ***

K. INTERCEPTION DE COURRIER ELECTRONIQUE

1. À l'instar du courrier postal ordinaire et des conversations téléphoniques, le courrier électronique devrait être considéré comme une communication privée. Les mesures législatives qui seront adoptées à la suite des présentes consultations devraient codifier clairement les attentes en matière de protection de la vie privée dans ce domaine, sauf lorsque les renseignements font l'objet d'une diffusion publique. *****

2. L'interception du courrier électronique devrait nécessiter une ordonnance judiciaire quel que soit le point d'interception. ****

3. Intercepter du courrier électronique alors qu'il est stocké chez un FSI équivaut à intercepter un message téléphonique enregistré dans une centrale locale de réception d'appels comme le service TéléRéponse de Bell. Il s'agit d'une communication privée qui devrait toujours être considérée comme telle. **

4. Obliger les FSI à stocker les messages électroniques pour une période de jusqu'à six mois soulève de sérieuses questions. Quelle garantie ont les citoyens que leurs messages électroniques seront effectivement supprimés au bout de six mois et comment le gouvernement garantira-t-il que les employés des FSI n'abuseront pas des dossiers de courrier électronique auxquels ils ont accès ? *

5. Il faut éviter d'insérer des détails techniques dans toute loi future portant sur l'interception du courrier électronique au risque de favoriser les querelles juridiques et les procès inutiles. ***

6. On devrait aussi s'assurer de tenir compte dans toute loi à venir, non seulement du courrier électronique, mais aussi d'outils de communications plus récents tels que le clavardage en temps réel et les services de messagerie. *

ANNEXE A

ORGANISMES ET ASSOCIATIONS CHARGES DE L'APPLICATION DE LA LOI AYANT REPONDU A LA DEMANDE DE CONSULTATION

	Organismes et associations chargés de l'application de la loi
1	Abbotsford Police Department
2	Barrie Police Service
3	Brantford Police Service
4	Brockville Police Service
5	Calgary Police Service
6	Association canadienne des chefs de police
7	Charlottetown Police Department
8	Chatham-Kent Police Service
9	Police du CN
10	Criminal Intelligence Service Alberta
11	Service de police de la ville de Laval
12	Durham Regional Police Service
13	Edmonton Police Service
14	Greater Sudbury Police Service
15	Guelph Police Service
16	Halton Regional Police Service
17	Hamilton Police Service
18	Lethbridge Police Service
19	London Police Service
20	New Liskeard Police Service
21	Niagara Regional Police Service
22	Oak Bay Police Department
23	Ontario Provincial Police / Police provinciale de l'Ontario
24	Ottawa Police Service / Service de police d'Ottawa

25	Oxford Community Police
26	Peterborough Lakefield Community Police Service
27	GRC – Calgary
28	GRC - Edmonton
29	GRC – Halifax
30	GRC – Kelowna
31	GRC – London
32	GRC – Montréal
33	GRC – Nouveau-Brunswick
34	GRC – Ottawa
35	GRC – Île-du-Prince-Édouard
36	GRC – Québec
37	GRC – Red Deer
38	GRC – Détachement du comté de Strathcona
39	GRC – Toronto
40	GRC – Vancouver
41	GRC – Whitehorse
42	Régie intermunicipale de police – Vallée du Richelieu
43	Regina Police Service
44	Royal Newfoundland Constabulary
45	Saint John Police Force
46	Saskatoon Police Service
47	Sault Ste. Marie Police Service
48	Sûreté municipale de Mont-Tremblant
49	Thunder Bay Police / Police de Thunder Bay

50	Timmins Police Service / Service de police de Timmins
51	Toronto Police Service / Service de police de Toronto
52	Truro Police Service
53	Vancouver Police Department
54	Waterloo Regional Police Service
55	Weyburn Police Service
56	Winnipeg Police Service / Service de police de Winnipeg

ANNEXE B

COMPAGNIES ET ASSOCIATIONS INDUSTRIELLES AYANT REPONDU A LA DEMANDE DE CONSULTATION

	Compagnies
1	Aliant Telecom Inc. BCE Inc. (Entreprises Bell Canada) MTS Communications Inc. Saskatchewan Telecommunications
2	Flora.ca
3	Microcell Telecommunications Inc.
4	Rogers Wireless AT&T
5	Telesat Canada
6	Telus
7	VeriSign Inc. (É.U.)
8	Yahoo Canada Co.

	Associations industrielles
1	Association des compagnies de Téléphone du Québec
2	Canadian Advisory Committee – Information Technology Security
3	Association canadienne des fournisseurs Internet
4	Association des banquiers canadiens
5	Association canadienne de télévision par câble
6	Chambre de commerce du Canada
7	Association canadienne de l'informatique
8	Canadian Public Policy Committee of the Computing Technology Industry Association
9	Association canadienne des télécommunications sans fil
10	Association canadienne de la technologie de l'information
11	Ontario Telecommunications Association
12	US Internet Service Provider Association (É.U.)

ANNEXE C

COMMISSAIRES A LA PROTECTION DE LA VIE PRIVEE ET A L'INFORMATION AYANT REPONDU A LA DEMANDE DE CONSULTATION

	Commissaires à la protection de la vie privée et à l'information
1	Commissaire à la protection de la vie privée du Canada
2	Commission d'accès à l'information du Québec
3	Information and Privacy Commissioner / Commissaire à l'information et à la protection de la vie privée de l'Ontario
4	Office of the Information and Privacy
5	Commissioner, Alberta Office of the Information and Privacy Commissioner for British Columbia

ANNEXE D

GROUPES DE LA SOCIETE CIVILE AYANT REPONDU A LA DEMANDE DE CONSULTATION

	Groupes de la société civile
1	B.C. Civil Liberties Association
2	British Columbia Freedom of Information and Privacy Association
3	Association du Barreau canadien
4	Association canadienne des libertés civiles
5	Canadian Library Association
6	Civil Liberties Association, NCR / Association des droits civils, région de la capitale nationale
7	Electronic Frontier Canada et Electronic Frontier Foundation (É.U.)
8	Internet Law Group- Université du Manitoba
9	Internet Law Group - University of Manitoba
10	Option consommateurs
11	PovNet
12	Privaterra - Computer Professionals for Social Responsibility
13	Public Interest Advocacy Centre / Centre pour la défense de l'intérêt public
14	Vancouver Community Network

ANNEXE E

MINISTERES
AYANT REPONDU A LA DEMANDE DE CONSULTATION

	Ministères
1	Ministère de la Justice de l'Alberta
2	Solliciteur général de l'Alberta