

Accès légal – Document de consultation

Ministère de la Justice
Industrie Canada
Solliciteur général du Canada

25 août 2002

Table des matières

INTRODUCTION	4
Un environnement qui évolue très rapidement	4
La <i>Convention sur la cybercriminalité</i> du Conseil de l'Europe	6
Objectifs de politique générale	7
Le processus de consultation	7
PROPOSITIONS LÉGISLATIVES	9
Infrastructure	9
Obligation de garantir la capacité d'interception	9
Exigences générales	10
Règlements	10
Exemption	11
Mécanisme de conformité	11
Coûts visant à garantir la capacité d'interception	12
Modifications au <i>Code criminel</i> et à d'autres lois	12
Ordonnances de production	12
Ordonnances générales de production	13
Ordonnances spécifiques de production	13
Ordonnances afin d'obtenir des données sur un abonné ou un fournisseur de service	15
Ordonnances d'assistance	16
Ordonnances de conservation	16
Propagation des virus informatiques	17
Interception du courrier électronique	18
Modifications à la <i>Loi sur la concurrence</i>	20
Autres moyens permettant de recueillir des renseignements sur les abonnés et les fournisseurs	21
CONCLUSION	22
Annexe 1 : Interception	24
Annexe 2 : Perquisition et saisie	26

INTRODUCTION

L'accès légal est une technique importante et bien implantée qui est utilisée par les organismes responsables de l'application de la loi et de la sécurité nationale pour mener des enquêtes. Dans le domaine des télécommunications au Canada, il s'agit de l'interception des communications et de la perquisition et la saisie de renseignements conformément au *Code criminel*, à la *Loi sur le Service canadien du renseignement de sécurité* et à d'autres lois fédérales comme la *Loi sur la concurrence*. Ces lois donnent aux organismes responsables de l'application de la loi et de la sécurité nationale le pouvoir d'intercepter les communications et de saisir les renseignements en conformité avec les droits et libertés garantis dans la *Charte canadienne des droits et libertés*, en particulier le droit à la protection contre les saisies et les perquisitions abusives. (On trouvera des renseignements supplémentaires sur l'interception et sur les saisies et perquisitions aux annexes 1 et 2 respectivement.)

Pour les organismes responsables de l'application de la loi et de la sécurité nationale, l'accès légal est un outil indispensable pour prévenir la criminalité, mener des enquêtes et poursuivre les criminels ayant commis des délits graves, ainsi que pour faire enquête sur les menaces à la sécurité du Canada. Les organismes d'application de la loi ont souvent recours à l'interception, à la perquisition et à la saisie de documents, de données informatiques et d'autres renseignements, conformément à la loi, dans le cadre d'enquêtes sur des crimes graves tels que le trafic de drogue, la pornographie juvénile, les meurtres, le blanchiment d'argent, les complots pour fixer les prix et le télémarketing trompeur. Les organismes responsables de la sécurité nationale ont aussi recours à l'interception, dans le respect de la loi, pour mener des enquêtes relatives au terrorisme et aux autres menaces pour la sécurité nationale. Selon le *Rapport annuel sur la surveillance électronique* du Solliciteur général, dans les cas où des preuves obtenues par interception légale sont produites, le taux de condamnations dépasse les 90 %.

De toute évidence, il est important de maintenir le principe et les pouvoirs de l'accès légal. Le défi est de le faire dans un contexte de changements technologiques rapides et dans le respect de la *Charte canadienne des droits et libertés*.

Un environnement qui évolue très rapidement

Les télécommunications et les réseaux informatiques modernes tels qu'Internet procurent nombre d'avantages économiques et sociaux, mais ils facilitent aussi la planification, la coordination, le financement et la perpétration de crimes et peuvent ainsi constituer une menace pour la sécurité du public et la sécurité nationale du Canada.

L'évolution rapide des moyens technologiques pose un défi de taille aux organismes d'application de la loi et de sécurité nationale devant avoir un accès légal aux communications et aux renseignements, car elle peut rendre plus difficile l'obtention des renseignements nécessaires pour pouvoir mener des enquêtes efficaces.

Alors que depuis 1996, les fournisseurs de certains services de communication sans fil, comme les services de communications personnelles, doivent être munis d'installations rendant possible l'accès légal en vertu d'une obligation qui figure dans la *Loi sur la radiocommunication*, il n'existe aucune obligation semblable pour les autres fournisseurs.

De nombreux nouveaux joueurs sont entrés sur le nouveau marché fébrile des télécommunications; cette nouvelle réalité, combinée à la multiplication des services rendue possible par la technologie, soulève régulièrement des problèmes en matière d'accès légal. De nos jours, aux fournisseurs de services téléphoniques avec fil s'ajoutent diverses sociétés de communications sans fil et un grand nombre de fournisseurs de services Internet, ce qui fait que les organismes d'application de la loi et de sécurité nationale doivent mener leurs enquêtes dans des conditions plus complexes.

Définition ad hoc – Fournisseur de services

Un fournisseur de services est une personne qui possède ou exploite des installations de transmission utilisées par elle-même ou par un tiers pour fournir des services de télécommunications au public au Canada.

Au cours des dernières années sont survenus plusieurs changements technologiques qui ont une incidence sur l'accès légal. Ces changements comprennent :

Communications avec fil : Les organismes d'application de la loi et de sécurité nationale mènent des enquêtes légales avec la collaboration des fournisseurs de services de communication depuis des années. Cependant, les options perfectionnées de service et les nouvelles caractéristiques d'appel compliquent le travail des enquêteurs.

Communications sans fil : La prolifération des appareils sans fil, notamment les téléphones cellulaires et téléphones numériques, tels que les services de communications personnelles et de communications par satellites, peut poser un problème important dans la mesure où l'infrastructure ne permet pas l'accès légal. Au rythme où les nouvelles technologies et services sans fil se répandent, il devient très difficile pour les organismes d'application de la loi et de sécurité nationale de continuer d'avoir les moyens techniques d'intercepter légalement les communications. En outre, ces technologies se généralisent à l'échelle mondiale, ce qui peut soulever d'importants problèmes de partage des compétences pendant les enquêtes criminelles et terroristes.

Internet : Internet est un regroupement de plus de 135 000 réseaux internationaux fonctionnant grâce à la commutation par paquets et pouvant échanger de l'information. Ce « réseau de réseaux » est totalement décentralisé et dénué de structure décisionnelle. La technologie sur laquelle reposent les communications

par Internet, la nécessité de disposer d'équipement de pointe pour pouvoir intercepter les communications conformément à la loi, de même que l'absence de dispositions obligeant les fournisseurs de services Internet à adopter des formules favorisant les activités légales d'interception sont autant de problèmes importants pour les enquêteurs.

À mesure que l'information et les communications sont transmises beaucoup plus rapidement partout dans le monde, les dispositions légales, les ententes et les techniques actuelles sont mises à rude épreuve. Les frontières ne jouent plus leur rôle à cet égard et il arrive de plus en plus souvent que les criminels ne résident pas où leurs actes produisent leurs effets. Compte tenu de ces changements, les organismes d'application de la loi et de sécurité nationale ont besoin de capacités modernes et efficaces pour mener leurs enquêtes et obtenir des renseignements. On envisage des dispositions législatives afin d'adapter le droit à l'état actuel de la technologie des télécommunications. Pour ce faire, et dans le but d'aider les organismes d'application de la loi et de sécurité nationale à être efficaces dans ce nouvel environnement, il est de plus en plus important de créer et de maintenir des partenariats avec l'industrie canadienne.

La Convention sur la cybercriminalité du Conseil de l'Europe

La *Convention sur la cybercriminalité* du Conseil de l'Europe est un traité international ayant pour but de fournir aux États signataires des moyens juridiques de faciliter les enquêtes et les poursuites relatives à la cybercriminalité, notamment aux crimes liés à l'utilisation d'Internet, de même que la production de preuves sous forme électronique pour ce genre de délits. Observateur permanent au Conseil de l'Europe, le Canada a été invité à participer à la négociation de la *Convention*. Au 12 août 2002, 33 pays avaient signé la *Convention*, y compris le Canada et la plupart des autres membres du G8.

La *Convention* demande la criminalisation de certaines infractions liées aux ordinateurs, l'adoption des pouvoirs nécessaires pour procéder aux enquêtes sur la cybercriminalité et poursuivre les coupables ainsi que la promotion de la coopération internationale par l'entraide juridique et l'extradition dans un domaine qui ne connaît pas de frontières. La *Convention* aidera le Canada et ses partenaires à être plus efficaces dans leur lutte contre les crimes visant l'intégrité, l'accessibilité et la confidentialité des systèmes informatiques et des réseaux de télécommunications et contre d'autres activités criminelles traditionnelles, telles que la fraude ou la distribution de pornographie juvénile, réalisées au moyen de ce genre de réseaux ou par Internet. La plupart des infractions et des formalités exigées existent déjà au Canada. Cependant, pour ratifier la *Convention* et la faire entrer en vigueur au Canada, il faudrait apporter les modifications suivantes au *Code criminel* :

- prévoir la possibilité de rendre une ordonnance de production;
- prévoir la possibilité de rendre une ordonnance de conservation;
- définir une infraction relative aux virus informatiques qui ne sont pas encore propagés.

Des modifications complémentaires ou d'autres modifications pourraient être apportées à d'autres lois existantes, telles que la *Loi sur la concurrence*, en vue de les rendre conformes à la *Convention*, notamment dans les domaines du repérage en temps réel des données relatives au trafic (voir plus loin la section portant sur les ordonnances spécifiques de production) et l'interception du courrier électronique.

On trouvera une explication et une description des propositions relatives à ces modifications ci-dessous.

Objectifs de politique générale

L'approche du gouvernement tient compte de la nécessité de protéger les droits, les renseignements personnels, la sécurité et le bien-être économique de tous les Canadiens et Canadiennes. Pour remplir leur mandat de sécurité publique, les organismes d'application de la loi et de sécurité nationale doivent conserver leurs possibilités d'accès légal sans contrevenir à la *Charte canadienne des droits et libertés*.

Conformément à l'engagement énoncé dans le Discours du trône de 2001 de fournir des outils modernes pour la lutte contre la cybercriminalité, ces propositions ont pour but de réviser le cadre juridique existant pour aider les organismes d'application de la loi et de sécurité nationale à relever les défis posés par les nouvelles technologies de communications et d'information.

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. Dans la poursuite de ces objectifs, on veille en outre à ce qu'aucune entrave à la compétitivité ne soit imposée aux entreprises canadiennes et que les solutions adoptées n'entraînent aucun fardeau indu pour la population canadienne.

Le processus de consultation

Le ministère de la Justice du Canada, de concert avec le Portefeuille du Solliciteur général du Canada et Industrie Canada, étudient différents moyens pour régler les problèmes liés à l'accès légal dans le cadre des technologies modernes des télécommunications et ont entrepris de consulter divers intéressés afin d'être mieux renseignés.

L'objectif du présent document est d'offrir à une gamme d'intervenants, notamment les provinces et les territoires, les organismes d'application de la loi et de sécurité nationale, les représentants du milieu des télécommunications et des secteurs connexes, les organismes de défense des libertés publiques et la collectivité juridique, l'occasion d'étudier des propositions visant la mise à jour des dispositions canadiennes sur l'accès légal. Celles-ci ont pour objet de répondre à trois besoins fondamentaux : 1) que les textes législatifs soient adaptés aux nouvelles technologies de télécommunications; 2) que les fournis-

seurs de services en télécommunications se dotent des moyens techniques permettant aux organismes responsables de l'application de la loi et de la sécurité nationale de recourir à l'accès légal; 3) que le Canada prenne les mesures législatives nécessaires pour ratifier la *Convention sur la cybercriminalité* du Conseil de l'Europe. Le tout donne suite à un examen global des lois ayant débuté en octobre 2000.

Les propositions contenues dans le présent document sont des points de départ en vue d'une discussion et les observations concernant l'une ou l'autre de ces propositions seront bienvenues.

PROPOSITIONS LÉGISLATIVES

Les propositions qui suivent traitent de l'obligation qu'auraient les fournisseurs de services de fournir la capacité technique permettant l'accès légal, ainsi que de la nécessité de rendre le *Code criminel* mieux adapté aux nouvelles technologies de télécommunications et de modifier le *Code criminel* et d'autres lois, telles que la *Loi sur la concurrence*, afin de permettre au Canada de ratifier la *Convention sur la cybercriminalité* du Conseil de l'Europe.

Plusieurs partenaires internationaux du Canada ont déjà mis à jour leur législation afin d'assurer aux organismes d'application de la loi et de sécurité nationale la possibilité de recourir à l'accès légal. La modernisation du cadre législatif est nécessaire pour que le Canada puisse continuer d'être un partenaire efficace sur le plan international et faire face aux défis posés par le développement actuel des technologies de télécommunications.

Infrastructure

Obligation de garantir la capacité d'interception

À l'heure actuelle, aucun mécanisme législatif ne peut être utilisé au Canada pour obliger les fournisseurs de services à développer ou à déployer des systèmes offrant une capacité d'interception, même si une autorisation judiciaire est obtenue par les organismes d'application de la loi et de sécurité nationale afin d'intercepter les communications d'une personne spécifique.

Il est proposé que tous les fournisseurs de services (avec fil, sans fil et fournisseurs de services Internet) soient tenus de s'assurer que leurs systèmes ont la capacité technique de fournir un accès légal aux organismes d'application de la loi et de sécurité nationale. La présente section traite de l'implantation et du maintien de cette infrastructure.

La proposition a pour principe fondamental que, conformément à une autorisation légale d'interception, les fournisseurs de services seraient contraints d'avoir la capacité technique permettant d'accéder à toutes les données spécifiques transmises par leurs installations, y compris celles relatives au contenu d'une télécommunication et les données relatives à cette même télécommunication.

Définition – Installation de transmission
« Installation de transmission » : fil, câble ou système radio, optique, électromagnétique ou autre système technique similaire utilisé pour transmettre de l'information entre les points d'arrivée d'un réseau.

Un nouveau texte législatif obligeant les fournisseurs de services à avoir des équipements de transmission permettant l'interception pourrait spécifier :

- les exigences fonctionnelles générales de la capacité d'interception;
- l'autorité réglementaire spécifiant les détails techniques des exigences fonctionnelles;
- le pouvoir d'exempter de certaines obligations;
- un mécanisme de conformité.

Exigences générales

La législation s'appliquerait à tous les fournisseurs de services de télécommunications qui opèrent une installation de transmission au Canada. Tous ces fournisseurs seraient tenus d'assurer au moins une capacité de base d'interception avant d'offrir au public un service nouveau ou nettement supérieur. Les exigences de la loi entreraient en vigueur à une date proclamée par le gouverneur en conseil (Cabinet).

Règlements

Il est essentiel que les fournisseurs de services sachent ce qu'on attend d'eux. La législation définirait les termes et préciserait l'approche globale et, conformément à celle-ci, le Cabinet pourrait, sur avis du ministre de l'Industrie et du Solliciteur général, prendre des règlements sur le fondement des pouvoirs qui seraient conférés par la loi. Les normes et les détails techniques seraient précisés dans les règlements.

La portée des règlements doit faire l'objet de discussions, mais pourraient inclure le pouvoir d'établir des normes ou des exigences techniques et autres applicables à un fournisseur de services. Les règlements pourraient décrire les moyens que pourraient prendre les fournisseurs de services pour permettre l'accès à leurs installations, les exigences en matière de sécurité sur le traitement des renseignements interceptés, les coûts et le mode d'élaboration des règlements mêmes.

Questions à examiner :

1. Comment les règlements pourraient-ils prescrire les normes ou exigences techniques et autres applicables :
 - a. à l'équipement qu'il faudra installer, annexer ou lier de quelque façon à ses installations et les exigences de capaci-

Définition – Équipement de transmission
 « Équipement de transmission » : tout équipement utilisé pour :

- a) procéder à la commutation de l'information transmise par télécommunication;
- b) l'entrée, la saisie, la conservation, l'organisation, la modification, l'extraction, la sortie ou tout autre traitement de l'information transmise par télécommunication;
- c) contrôler la vitesse, le code, le protocole, le contenu, le format, l'acheminement ou tout autre aspect similaire de la transmission de l'information par télécommunication.

- té relativement au nombre maximal d'interceptions simultanées sur cet équipement?
- b. aux modalités et aux conditions relatives à la sécurité des interceptions et de la transmission du résultat des interceptions?
 - c. à la compétence, la fiabilité et la mise en place du personnel?
2. Les règlements devraient-ils prévoir les frais à payer à un fournisseur de services pour l'assistance opérationnelle?

Avant de recommander l'adoption d'un règlement au Cabinet, le ministre de l'Industrie, de même que le Solliciteur général, consulteraient les représentants de personnes appropriées dont les intérêts seraient touchés par le règlement.

Exemption

Étant donné que l'obligation de garantir la capacité d'interception s'appliquerait à tous les fournisseurs de services, la législation doit être flexible et il doit être possible de l'adapter à des situations particulières. Un système d'exemption constituerait un mécanisme permettant d'obtenir de la flexibilité et d'éviter des problèmes tels que la création de zones où l'interception ne serait pas possible. Ce système éliminerait l'obligation de respecter la loi ou le règlement en tout ou en partie, pour une durée limitée.

L'exemption pourrait fonctionner de la façon suivante, aux fins de la discussion : le Cabinet aurait le pouvoir d'exempter et de déléguer ce pouvoir conjointement au Solliciteur général et au ministre de l'Industrie. Les deux ministères prépareraient les lignes directrices administratives qui s'appliqueraient au traitement des demandes d'exemption et ces lignes directrices seraient mises à la disposition du public. Pendant que les ministres examineraient une demande d'exemption, le fournisseur de services ne serait pas assujéti à une pénalité.

Mécanisme de conformité

Des dispositions en matière de conformité permettraient de s'assurer de l'effectivité des textes législatifs et de l'existence d'un mécanisme par lequel les fournisseurs de services pourraient s'assurer qu'ils respectent la loi. Ces dispositions pourraient autoriser ou exiger des inspections ou des analyses. Néanmoins, les mécanismes recherchés devraient viser à minimiser les coûts à la fois pour l'industrie et le gouvernement.

Questions à examiner :

- Quelle sorte de mécanisme de conformité faudrait-il?
- Qui devrait procéder aux activités de conformité et déterminer les circonstances dans lesquelles elles peuvent s'appliquer?
- Quel type de pénalité devrait être prévu dans les cas où les fournisseurs de services ne respecteraient pas la loi?

Coûts visant à garantir la capacité d'interception

Le gouvernement recherche de quelle façon les coûts pourraient être répartis selon un régime qui couvrirait trois grands cas de figures. À compter d'une date restant à définir par le Cabinet :

1. les fournisseurs de services seraient tenus responsables des coûts de l'accès légal lorsqu'ils introduiraient de nouvelles technologies ou de nouveaux services, et
2. les fournisseurs de services seraient tenus responsables des coûts de l'accès légal en cas d'amélioration significative de leur système ou réseau; toutefois,
3. les fournisseurs de services ne seraient pas tenus d'apporter des modifications à leurs systèmes ou réseaux existants à leurs propres frais.

Modifications au *Code criminel* et à d'autres lois

Plusieurs modifications à des lois telles que le *Code criminel* ont été proposées afin que les textes législatifs soient adaptés aux nouvelles technologies de télécommunications et pour permettre au Canada de ratifier la *Convention sur la cybercriminalité* du Conseil de l'Europe.

Ordonnances de production

Une ordonnance de production exige que le possesseur des documents remette ces documents à certaines personnes (comme les agents chargés d'appliquer la loi) dans un délai précis, ou les mette à leur disposition. Les ordonnances de production sont déjà prévues dans certaines lois fédérales, telles que la *Loi sur la concurrence*. Cependant, sauf pour certains types d'ordonnances de production et de cueillette dont la portée est restreinte, le *Code criminel* ne prévoit pas ce type d'ordonnance.

Trois propositions législatives sont à l'étude afin de conférer aux organismes d'application de la loi des pouvoirs de nature procédurale qui leur permettraient de faire face aux nouvelles technologies :

- une ordonnance générale de production;
- une ordonnance spécifique de production des données relatives au trafic;
- une ordonnance spécifique de production des données sur les abonnés ou fournisseurs de services.

En créant soit une ordonnance de production générale ou une ordonnance de production spécifique, il serait essentiel de maintenir et de reconnaître les droits protégés par la *Charte canadienne des droits et libertés*, notamment la protection de chacun contre l'auto-incrimination.

Ordonnances générales de production

Lorsqu'il s'agit d'une perquisition effectuée chez un tiers, notamment une société ou une banque, il arrive qu'un organisme d'application de la loi obtienne un mandat de perquisition du tribunal mais qu'il n'effectue pas lui-même la perquisition. Pour des raisons d'ordre pratique, c'est souvent le tiers en possession des documents qui est le mieux placé pour les produire et qui le fait. Toutefois, ce dernier aura peut-être besoin d'un délai pour trouver et produire les documents à l'organisme d'application de la loi.

On pourrait résoudre ce problème en créant une ordonnance générale de production qui exigerait du possesseur qu'il produise ou rende disponibles les documents à des agents responsables de l'application de la loi dans un délai précis. L'ordonnance pourrait être rendue dans des circonstances semblables à celles qui entourent le mandat de perquisition. L'exécution d'une telle ordonnance serait probablement considérée comme étant moins intrusive qu'un mandat de perquisition puisque l'organisme d'application de la loi n'aurait pas à s'introduire dans les locaux du tiers afin d'y effectuer la fouille. L'ordonnance permettrait également aux organismes d'application de la loi d'obtenir des documents lorsque, en raison du fait que les documents sont stockés dans un État étranger, il n'est pas possible d'obtenir un mandat de perquisition.

Questions à examiner :

- Faut-il modifier le *Code criminel* pour permettre aux organismes d'application de la loi d'obtenir une ordonnance de production dans certaines situations?
- Faut-il prévoir dans le *Code criminel* des ordonnances anticipatoires (permettre aux organismes d'application de la loi de surveiller les transactions pendant un certain temps)?
- Quelles devraient être les garanties procédurales?

Ordonnances spécifiques de production

Aux termes du *Code criminel*, il n'est pas permis aux organismes d'application de la loi d'obtenir des documents ou des renseignements sans avoir des motifs raisonnables de croire qu'une infraction a été ou sera commise. Cette exigence permet à la fois de tenir compte du fait que l'État doit être en mesure d'obtenir la preuve de la perpétration d'un crime et les intérêts relatifs à la protection de la vie privée de la personne qui détient l'information. L'exigence est particulièrement opportune lorsque l'attente est très élevée en matière de vie privée, notamment quand il s'agit du contenu d'un document privé. Toutefois, le *Code criminel* prévoit aussi la possibilité que le tribunal se fonde sur un critère moins exigeant dans certains cas afin d'ordonner la production ou l'obtention de documents, par exemple lorsqu'il s'agit de renseignements fiscaux relativement à certaines infractions, d'appareils de localisation ou d'enregistreurs de numéros signalés (appareils enregistrant les numéros d'appels entrant et sortant), au tout début d'une enquête. Sauf dans ces quelques rares cas, la mesure de protection ne permet pas d'obtenir des rensei-

gnements importants au début d'une enquête, même si l'attente est faible en matière de vie privée en ce qui a trait à l'information recherchée.

Une ordonnance spécifique de production comportant un critère moins contraignant pourrait être créée afin de permettre la production de données relatives aux télécommunications, qui s'ajouterait à l'article 492.2 du *Code criminel* qui traite des enregistreurs de numéros de téléphone et aux dispositions relatives à la cueillette en temps réel ou historique de données relatives au trafic. Le *Code criminel* actuel autorise la recherche

Définition – Données relatives aux télécommunications

« Données relatives aux télécommunications » : toute donnée, y compris les données relatives aux fonctions de composition, d'acheminement, d'adressage ou de signal qui identifient ou visent à identifier l'origine, la direction, l'heure, la durée ou la taille, selon le cas, ainsi que le destinataire ou le point d'arrivée d'une transmission par télécommunication, générée ou reçue au moyen de l'installation de télécommunications exploitée par le fournisseur de service ou une installation lui appartenant.

de données relatives au trafic en temps réel en vertu de l'article 487.01 ou de la Partie VI, mais le critère applicable aux données relatives au trafic électronique devrait s'apparenter davantage au critère applicable aux appels enregistrés et aux enregistreurs de numéros signalés compte tenu de l'attente moins élevée en matière de vie privée pour ce qui est d'un numéro de téléphone ou d'une adresse Internet, par opposition au contenu d'une communication.

On pourrait également créer une ordonnance spécifique de production comportant un critère moins contraignant qui permette d'obtenir d'autres données ou informations à l'égard desquelles l'attente est moins élevée en matière de respect de la vie privée.

Questions à examiner :

- Faut-il prévoir un pouvoir précis, semblable à celui qui s'applique dans le *Code criminel* aux enregistreurs de numéros signalés, pour permettre aux organismes d'application de la loi et de sécurité nationale d'obtenir des données relatives au trafic?
- Comment devrait-on définir « données relatives au trafic »? La définition des données relatives au trafic doit-elle être associée aux informations d'ordre téléphonique et traitées dans le même article du *Code criminel*?
- Faut-il créer d'autres types d'ordonnances spécifiques de production comportant un seuil moins élevé?
- Quelles seraient les garanties procédurales à inclure?

Ordonnances afin d'obtenir des données sur un abonné ou un fournisseur de service

Par le passé, les fournisseurs de services divulguaient les données de base sur un client, notamment le nom, l'adresse de facturation, le numéro de téléphone et le nom du fournisseur de services, sans autorisation légale préalable (par exemple, sans mandat de perquisition). Cette façon de procéder était conforme à la décision de la Cour suprême du Canada dans *R. c. Plant*, (1993) 3 R.C.S. 281, dans laquelle la Cour a dit que, dans le contexte d'un renseignement détenu par une entreprise, une personne ne peut raisonnablement s'attendre au respect de sa vie privée à l'égard de renseignements qui ne révèlent pas des détails intimes sur son mode de vie et ses choix personnels. La *Loi sur la protection des renseignements personnels et les documents électroniques* permet la communication de ces renseignements personnels sans la connaissance et le consentement de l'individu visé si la communication est demandée par un organisme gouvernemental qui a fait la preuve de son pouvoir légal d'obtenir ces renseignements.

De plus, en ce qui concerne les renseignements relatifs aux noms et adresses de l'abonné (NAA), le Conseil de la radiodiffusion et des télécommunications (CRTC) a décidé qu'il n'exercerait pas les pouvoirs dont il dispose pour de telles informations confidentielles; il examine actuellement la possibilité de confier à certains fournisseurs de service la recherche inversée pour des informations non confidentielles concernant le nom ou l'adresse du client. Conformément à des décisions récentes du CRTC, les renseignements qui permettent de déterminer l'identité d'un fournisseur de services locaux ne peuvent être fournis que sous certaines conditions.

Toutefois, si ces conditions n'ont pas été respectées ou si le gardien des renseignements refuse de collaborer, l'organisme d'application de la loi n'a aucun moyen d'exiger la production de renseignements relatifs au client ou à l'abonné en l'absence d'une ordonnance du tribunal à cette fin. Le problème est encore plus grave lorsqu'il est impossible d'obtenir un mandat en vertu du *Code criminel* (p. ex., l'article 487), parce que l'organisme d'application de la loi peut vouloir demander ces renseignements pour des raisons qui ne sont pas reliées à l'enquête (p. ex., pour localiser le plus proche parent en cas d'urgence) ou parce qu'il n'en est qu'au début de son enquête.

Questions à examiner :

- Faut-il une ordonnance spécifique de production du nom et de l'adresse du client, de même que des données du fournisseur de service?
- Sous quelles conditions de tels renseignements doivent-ils être rendus accessibles, et à qui?
- Quel seuil doit s'appliquer?
- Faut-il imposer cette obligation même si le fournisseur de services ne recueille pas présentement ces renseignements à ses propres fins?

Ordonnances d'assistance

L'article 487.02 du *Code criminel* prévoit qu'un juge ou un juge de paix qui accorde une autorisation d'intercepter une communication privée, qui décerne un mandat ou qui rend une ordonnance autorisant l'utilisation d'un enregistreur de numéros peut également rendre une ordonnance exigeant d'une personne qu'elle prête son assistance à l'exécution de ces ordonnances. De telles ordonnances d'assistance ne peuvent être rendues que si l'assistance peut raisonnablement être jugée nécessaire à l'exécution de ces ordonnances.

Certains agents responsables de l'application de la loi ont soulevé la possibilité d'inclure les ordonnances d'assistance dans d'autres lois, telles que la *Loi sur la concurrence*, qui permettent déjà de décerner des mandats ou de donner des autorisations d'interception. Certains intéressés ont également suggéré que toute loi qui permet de donner des ordonnances d'assistance devrait indiquer clairement ce qui pourrait être exigé précisément en vertu de telles ordonnances. Dans le contexte de l'accès légal, de telles clarifications dans la loi permettraient aux fournisseurs de services de comprendre plus clairement l'étendue de leurs obligations.

Questions à examiner :

- Les textes législatifs qui permettent déjà de décerner des mandats ou d'accorder des autorisations d'interception devraient-ils être modifiés pour prendre en considération la possibilité pour un juge ou un juge de la paix d'accorder une ordonnance d'assistance en vue de l'exécution du mandat ou de l'autorisation?
- Les ordonnances d'assistance devraient-elles indiquer de façon plus précise la portée et les limites de l'assistance requise d'une personne pour permettre l'exécution du mandat ou de l'autorisation?

Ordonnances de conservation

Il y a dans la *Convention sur la cybercriminalité* du Conseil de l'Europe un mécanisme procédural qui n'existe pas en droit interne canadien : c'est l'ordonnance de conservation. Il s'agit d'une ordonnance judiciaire qui exige du fournisseur de services visé par l'ordonnance qu'il stocke et conserve toutes les données existantes qui se rapportent à une transaction ou à un client spécifique. Il s'agit d'une mesure temporaire qui serait en vigueur seulement pour la durée nécessaire afin de permettre à l'organisme d'application de la loi d'obtenir un mandat l'autorisant à saisir les données ou une ordonnance de production des données. Par exemple, dans le cas d'un fournisseur de services Internet (FSI), une ordonnance de conservation pourrait obliger ce dernier à ne pas supprimer de renseignements précis en rapport avec un abonné en particulier. Il s'agit d'une mesure provisoire qui permet d'assurer que les renseignements essentiels en rapport avec une enquête particulière ne soient pas supprimés avant l'obtention par l'organisme d'application de la loi d'un mandat de perquisition ou d'une ordonnance de production.

Il est également proposé que dans certaines circonstances, l'organisme d'application de la loi puisse imposer au fournisseur de services l'obligation de conserver des données sans ordonnance judiciaire pour une période déterminée (par exemple quatre jours), si les conditions applicables à l'obtention d'une ordonnance judiciaire sont respectées mais qu'à cause de circonstances extraordinaires, il serait à peu près impossible d'obtenir l'ordonnance. Le *Code criminel* contient déjà une disposition sur les circonstances exceptionnelles en rapport avec les mandats de perquisition et l'écoute électronique.

Soulignons que la conservation des données se distingue du stockage des données. La conservation des données est ordonnée, tel que susmentionné, par le tribunal et l'ordonnance est signifiée à un fournisseur de services afin *de protéger l'intégrité d'un renseignement existant précis en rapport avec un abonné particulier*. Par contre, le stockage des données est une exigence générale selon laquelle les fournisseurs de services pourraient être tenus de *recueillir et de stocker certaines données concernant tous leurs abonnés*.

Questions à examiner :

- L'ordonnance de conservation devrait-elle s'appliquer seulement aux données emmagasinées dans les ordinateurs ou devrait-elle s'appliquer aussi aux documents papiers?
- Quel critère devrait servir à déterminer si l'ordonnance de conservation doit être accordée?
- Le critère devrait-il varier en fonction de la nature des données?
- Qui devrait pouvoir autoriser une ordonnance de conservation?
- Quelle est la période raisonnable pendant laquelle le gardien des données devrait être forcé de conserver les données : 90, 120 ou 180 jours?
- Devrait-il exister une peine spécifique pour le non-respect d'une ordonnance de conservation, ou l'outrage au tribunal est-il suffisant?
- Quelle est la période pendant laquelle l'agent d'application de la loi devrait être habilité à imposer une ordonnance de conservation aux fournisseurs de services dans des circonstances exceptionnelles?

Propagation des virus informatiques

En vertu des dispositions actuelles du *Code criminel*, seuls les effets de la propagation d'un virus informatique ou la tentative de propagation d'un tel virus constituent des infractions. En 1985, lorsque les dispositions relatives à l'utilisation non autorisée d'un ordinateur ont été adoptées, des modifications connexes ont été apportées aux dispositions du *Code criminel* sur le méfait afin que tout acte perpétré à l'aide d'un système informatique qui constitue un méfait constitue également une infraction en vertu des lois canadiennes.

La *Convention sur la cybercriminalité* du Conseil de l'Europe exige que les États signataires criminalisent la création, la vente et la possession sans autorisation, d'appareils (p. ex, programmes informatiques) conçus ou adaptés en vue principalement de perpétrer les

infractions précisées dans la Convention, que le virus ait ou non été disséminé ou qu'il ait ou non causé des dommages. Le *Code criminel* ne fait pas cette distinction. Il faudrait modifier légèrement les termes de l'article 342.2 afin de clarifier le fait que la création, la vente et la possession d'un programme-virus aux fins de perpétrer un cybercrime ou un méfait constituent une infraction en droit canadien.

En outre, afin de ratifier la *Convention*, il faudrait ajouter de nouvelles infractions relatives aux dispositifs illégaux (comme les virus). Il s'agit de l'importation, de l'achat à des fins d'utilisation et de la mise à disposition d'un dispositif illégal au sens de la *Convention*.

Interception du courrier électronique

Les dispositions de la Partie VI du *Code criminel* interdisent d'intercepter volontairement une « communication privée » et proposent un régime permettant d'obtenir une autorisation judiciaire afin d'intercepter ces communications. (Vous trouverez dans l'annexe 1 une description des dispositions actuelles du *Code criminel* sur l'interception.) Les critères applicables pour pouvoir intercepter une « communication privée » sont plus sévères que ceux relatifs à l'obtention d'un mandat de perquisition permettant de saisir des documents ou des dossiers (Voir l'annexe 2). Aux termes de l'article 183, Partie VI du *Code criminel*, une « communication privée » est une communication *orale* ou télécommunication faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La disposition semble supposer que lorsqu'une communication est consignée par écrit, il ne s'agit plus réellement d'une « communication privée » aux fins des dispositions relatives à l'interception des communications en vertu du *Code criminel*.

De fait, certains tribunaux ont déclaré qu'un message enregistré, à l'instar d'une lettre, n'était pas visé par la définition de l'expression « communication privée » parce qu'il n'était pas raisonnable que la personne qui envoie l'enregistrement (ou la lettre) s'attende à ce que son contenu demeure tout à fait privé. Puisqu'il s'agissait d'une inscription permanente du contenu, le document pouvait facilement se retrouver entre les mains d'un tiers. Suivant ce raisonnement, on pourrait prétendre qu'un courrier électronique, qui est un écrit, ne serait pas visé par la définition de l'expression « communication privée ». Par conséquent, ces documents écrits pourraient être obtenus par mandat de perquisition.

Toutefois, dans certaines affaires relatives au courrier électronique au Canada, les tribunaux ont jugé qu'il s'agissait de « communications privées ». Par exemple, un juge en Alberta a récemment conclu qu'il fallait obtenir l'autorisation judiciaire prévue par la Partie VI afin d'intercepter du courrier électronique puisque les expéditeurs et les destinataires pouvaient raisonnablement s'attendre au respect de leur vie privée.

Ces décisions, de même que la définition de l'expression « communication privée », créent une certaine confusion en ce qui a trait à la saisie ou à l'interception du courrier électronique. Le problème est attribuable au fonctionnement de cette technologie de

« stockage et transmission » de la communication. En fait, il est possible de prendre connaissance d'un courrier électronique en divers lieux ou à diverses étapes du processus de communication ou de transmission par diverses techniques. Les étapes suivantes du processus de communication ou de transmission pourraient probablement être qualifiées « d'interceptions » :

- pendant la saisie au clavier par l'expéditeur du message;
- pendant la transmission du message entre l'ordinateur de l'expéditeur et son FSI;
- pendant la transmission du message entre le FSI de l'expéditeur et celui du destinataire;
- pendant la transmission du message entre le FSI du destinataire et l'ordinateur du destinataire;
- pendant la réception du message de l'expéditeur par le destinataire.

La façon dont le courrier électronique est transmis, la relation entre la transmission et la réception du message, et l'action réciproque entre l'expéditeur et le destinataire semblent correspondre à la définition actuelle du terme « intercepter » dans le *Code criminel*.

Deux étapes posent davantage de problèmes :

- pendant le stockage du courrier électronique chez le FSI de l'expéditeur;
- pendant le stockage du courrier électronique chez le FSI du destinataire.

Dans ces circonstances, l'acquisition du courrier électronique peut, à l'occasion, se faire en même temps que la transmission du courrier, mais elle peut également être reportée à plus tard. En outre, le courrier peut être stocké pendant de longues périodes de temps (des semaines ou des mois) avant d'être ouvert par le destinataire. La transmission et l'acquisition simultanées du contenu d'un courrier électronique pourraient constituer une forme « d'interception » en vertu de la Partie VI du *Code criminel*. Toutefois, l'acquisition de ces contenus une fois stockés pourrait aussi constituer une « saisie » en vertu de la Partie XV du *Code criminel* ou des articles 15 et 16 de la *Loi sur la concurrence*.

Un dernier cas de figure pose également problème : la saisie d'un courriel ouvert chez le FSI du destinataire.

Cette situation ressemble au cas d'une personne qui, après avoir lu une lettre, la dépose dans un classeur plutôt que de la jeter aux poubelles. L'obtention du courriel à cette étape ressemble davantage à une saisie qu'à une interception.

Le principal problème au Canada est celui que pose l'examen du contenu d'un courrier électronique en transit chez un tiers ou en attente de livraison, ce qui pourrait constituer l'« interception » d'une « communication privée » au sens du *Code criminel*, quel que soit le moment de l'examen. D'autres toutefois prétendent que l'acquisition d'un courriel

dans ces circonstances constitue une « perquisition ou une saisie ». La question se pose à savoir si le *Code criminel* et d'autres lois, telles que la *Loi sur la concurrence*, devaient être modifiées pour indiquer de façon plus claire le type d'ordonnance à obtenir avant de pouvoir accéder à un courriel.

Questions à examiner :

- Faut-il prévoir une disposition précise au *Code criminel* sur le mode d'acquisition d'un courriel électronique?
- Le cas échéant, quelles seraient les garanties procédurales souhaitables?
- Devrait-on prévoir divers types d'ordonnances relatives au courriel électronique selon l'étape de la communication ou du processus de livraison?

Modifications à la *Loi sur la concurrence*

En plus des besoins propres aux organismes d'application de la loi, tels que les modifications proposées relatives aux ordonnances de conservation et celles visant à obtenir des renseignements sur un abonné ou un fournisseur de services dont il est question précédemment, le Bureau de la concurrence fait face à de nouveaux défis technologiques importants qui ont une incidence sur sa capacité d'avoir un accès légal aux éléments de preuve pour les infractions en vertu de la *Loi sur la concurrence*.

Les pratiques commerciales dolosives, le télémarketing frauduleux et les autres fraudes visant des consommateurs, la fixation des prix et le truquage des offres sont autant d'infractions aux règles de la concurrence qui peuvent être facilitées par les systèmes informatiques et les télécommunications. Les éléments de preuve pour ces types d'infractions sont de plus en plus de nature électronique et de grandes quantités de données peuvent être stockées dans des appareils ou sur des médias de plus en plus petits. En outre, le type de criminels qui commettent certaines de ces infractions criminelles change. Par exemple, en télémarketing, les pseudonymes sont fréquemment utilisés et il existe un lien de plus en plus important entre les éléments criminels associés à ce type d'activité et les menaces à la sécurité des Canadiens et Canadiennes.

On compte parmi les pouvoirs d'enquête du Bureau de la concurrence les ordonnances de production, les perquisitions et saisies et les interceptions de communications privées. Pour lui permettre de continuer à être en mesure d'accéder légalement au type d'éléments de preuve dont il a besoin pour remplir son mandat, il a été proposé que des amendements soient apportés à *Loi sur la concurrence*, dont les suivants :

Accès à des éléments cachés

Cet accès permettrait de demander aux personnes qui se trouvent sur les lieux d'une perquisition de fournir aux agents sur les lieux tout élément qu'elles cachent sur elles, notamment les appareils et les médias électroniques et numériques, et qui est mentionné

dans le mandat de perquisition, et prévoierait une disposition relative à l'entrave devant s'appliquer à ceux qui refusent de collaborer.

Autres ordonnances

Ces ordonnances permettraient d'obtenir des mandats généraux et des ordonnances d'assistance, ce qui améliorerait l'efficacité des outils de rassemblement des éléments de preuve.

Autres moyens permettant de recueillir des renseignements sur les abonnés et les fournisseurs

Les organismes d'application de la loi et de sécurité nationale doivent disposer de renseignements précis sur les personnes visées par une enquête afin de déterminer où ils doivent intercepter une communication. Les organismes d'application de la loi doivent aussi disposer de ces renseignements afin de pouvoir obtenir un mandat de perquisition.

Depuis la déréglementation du marché des télécommunications, le réseau téléphonique est devenu si complexe que les organismes d'application de la loi et de sécurité nationale éprouvent des difficultés et doivent consacrer beaucoup de temps à identifier le fournisseur de services locaux. Trouver de l'information sur l'identité du fournisseur de services locaux (IFSL) est la première étape de l'identification d'un abonné à partir de son adresse ou de son numéro de téléphone. Toutefois, pour obtenir ces renseignements, il n'y a qu'un seul moyen : contacter directement chaque fournisseur local, ce qui constitue un processus long et coûteux.

Le CRTC a récemment approuvé les conditions sous lesquelles Bell Canada pourra communiquer des renseignements sur l'identité du fournisseur de services locaux (IFSL) (<http://www.crtc.gc.ca/archive/FRN/Decisions/2002/dt2002-21.htm>) sans ordonnance du tribunal en cas d'urgence, pour des raisons d'application de la loi et de sécurité nationale. Le service d'identification du fournisseur de services local fourni par Bell Canada apporterait en partie une solution aux problèmes soulevés, notamment par les organismes d'application de la loi, en ce qui a trait à l'accès à des renseignements précis en temps opportun.

De façon connexe, se pose également le problème de la manière dont les organismes d'application de la loi et de sécurité nationale peuvent obtenir l'accès aux noms et à l'adresse de l'abonné, sachant que certains fournisseurs de services ne conservent ni ne détiennent de tels renseignements. Le CRTC a décidé qu'il n'exercerait pas les pouvoirs dont il dispose au sujet des renseignements liés aux noms et adresses confidentiels des abonnés. Il tente également de déterminer à l'heure actuelle si certains fournisseurs de services de communications avec fil devraient avoir le pouvoir d'effectuer des recherches inversées pour des informations non confidentielles concernant le nom et l'adresse du client.

Certains États, notamment l’Australie, les Pays-Bas et l’Allemagne, ont créé des bases de données ou des moyens légaux permettant aux organismes d’application de la loi et de sécurité nationale d’accélérer le processus d’obtention de renseignements précis sur un abonné et sur son fournisseur de services. Dans ces pays, les fournisseurs de services de télécommunications sont tenus de donner ces renseignements et d’en assurer la précision, l’intégralité et la fiabilité.

L’Association canadienne des chefs de police a formulé des recommandations afin d’améliorer l’accès légal à ces renseignements, notamment la création d’une base de données nationale. L’utilisation de cette base de données supposerait que les fournisseurs de services seraient tenus de la tenir à jour par des renseignements précis et pertinents. D’autres options, telles que le recours à des sources de renseignements existantes comme les bases de données du service « 911 » ou les répertoires téléphoniques privés, pourraient aussi être envisagées. Ces options devraient être utilisées en conformité avec la *Loi sur la protection des renseignements personnels*, la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* et toute autre loi applicable.

Questions à examiner :

- Quels types de moyen devraient être mis en place pour permettre aux organismes d’application de la loi et de sécurité nationale d’obtenir des renseignements à jour sur le NAA et l’IFSL tout en respectant le droit à la vie privée des Canadiens et Canadiennes?
- Une obligation de recueillir de tels renseignements sur le NAA devrait-elle être imposée, même si le fournisseur de services de télécommunications ne recueille pas ces renseignements pour son propre usage? En d’autres mots, les fournisseurs devraient-ils être forcés par la loi à recueillir les renseignements relatifs au NAA?
- Certains moyens ont déjà été mis en place dans le monde de la téléphonie, au sujet des renseignements relatifs à l’abonné (NAA). Certains de ces moyens devraient-ils être utilisés afin de permettre l’obtention de renseignements semblables sur l’abonné pour les fournisseurs de services Internet?
- Qui assumera les frais de la collecte, de la conservation et de la consultation de ces renseignements?
- Si une base de données était créée, quel organisme devrait être chargé de sa gestion?

CONCLUSION

Les fonctionnaires du gouvernement du Canada se proposent de rencontrer un éventail de parties intéressées pendant l’automne 2002 pour discuter des questions abordées dans le présent document. Vos observations sont bienvenues. Elles permettront au gouvernement d’élaborer une réponse appropriée à ces questions.

Le présent texte et d’autres documents relatifs aux consultations sont disponibles sur le site Internet du ministère de la Justice à l’adresse

http://www.canada.justice.gc.ca/fr/cons/la_al. On peut envoyer ses commentaires, par courrier électronique, à l'adresse suivante la-al@justice.gc.ca ou en utilisant le lien courriel sur le site Internet du ministère. Les commentaires peuvent aussi être envoyés par courrier à :

Consultation sur l'accès légal
Section de la politique en matière de droit pénal
284 Wellington
5^{ème} étage
Ottawa, Ontario, Canada, K1A 0H8.

Prière d'envoyer toute observation d'ici le 15 novembre 2002 afin d'assurer sa prise en considération.

Annexe 1 : Interception

Les dispositions prévues par ce qui constitue désormais la Partie VI du *Code criminel* sont entrées en vigueur il y a plus de 28 ans, soit le 1^{er} juillet 1974. Ces dispositions protègent la vie privée des Canadiens et Canadiennes en considérant comme une infraction le fait d'intercepter des communications privées, hors les cas prévus par la loi, tout en procurant à la police les moyens d'obtenir les autorisations légales nécessaires aux enquêtes criminelles. Les conditions requises pour l'obtention d'une autorisation en vertu de l'article 185 et d'un mandat en vertu de l'article 487.01 sont définies dans les Parties VI et XV du *Code criminel*.

Les principales caractéristiques de ces conditions sont les suivantes :

- Un enquêteur de police doit signer un affidavit indiquant sous serment les faits qui le justifient de penser qu'une autorisation ou un mandat doivent être délivrés; il doit également indiquer quels motifs raisonnables le fondent à penser que la surveillance électronique de certaines personnes ou la fouille de certains lieux pourrait être utile à l'enquête.
- L'agent désigné est chargé de s'assurer que tous les éléments liés à la demande d'autorisation sont conformes à la loi. Par ailleurs, il doit certifier que l'infraction, réprimée par la loi, est de caractère suffisamment grave pour justifier une telle demande, et que les preuves actuelles ne suffisent pas à prouver l'infraction.
- Dans le cas d'une demande faite en vertu de l'article 185, lorsqu'il étudie la demande, le juge doit être convaincu que la délivrance de l'autorisation servira au mieux les intérêts de l'administration de la justice, et que d'autres modes d'enquête ont été tentés mais en vain, ou qu'aucun autre procédé n'est susceptible de réussir, ou encore que l'affaire présente un caractère d'urgence telle qu'il ne serait pas pratique de recourir uniquement à d'autres procédés. Aucune de ces dernières conditions ne s'applique dans le cas, restreint, des organisations criminelles. Le juge peut également exiger que diverses conditions soient respectées au moment de la mise en application de l'autorisation s'il le juge opportun.

Les principales caractéristiques du régime procédural de l'article 185 sont les suivantes :

- Seul le Solliciteur général, ou les personnes spécialement désignées par celui-ci, peuvent formuler une demande d'autorisation pour des infractions devant être poursuivies au nom du gouvernement du Canada. Dans la pratique, les demandes sont faites par les avocats employés par le ministère fédéral de la Justice ou mandataires de ce dernier qui sont désignés par le Solliciteur général et, dans le cas de demandes d'autorisation urgentes, par des officiers de police supérieurs, eux aussi spécialement désignés par le Solliciteur général.

- Les agents de la paix peuvent exiger que l'agent désigné ne fasse une demande qu'après avoir reçu l'accord écrit d'un officier supérieur de leur organisme d'application de la loi respectif.

Annexe 2 : Perquisition et saisie

Une perquisition, c'est l'enquête, dans un lieu donné, visant à découvrir quelque chose ou à réunir des preuves d'une infraction à la loi, afin de les utiliser pour des poursuites. La saisie, lorsqu'elle survient au cours d'une perquisition, peut être définie comme une « saisie de bien(s) pour les besoins d'une enquête ou d'une recherche de preuves ».

L'idée à la base de ces deux définitions est celle d'un examen approfondi sur place, en général dans un but pénal. Le pouvoir d'effectuer une recherche de renseignements, de mener une enquête ou d'opérer une saisie implique un examen méthodique des lieux par un agent de l'État qui, ayant des motifs raisonnables de croire qu'il y a eu infraction à la loi, cherche des preuves de cette infraction. Un tel examen minutieux est entrepris dans le but de supprimer les infractions à la loi et d'en sanctionner les auteurs.

Sauf dans des circonstances exceptionnelles, par exemple lorsque l'urgence en rend impossible l'obtention, les perquisitions et les saisies sont effectuées en vertu d'un mandat de perquisition obtenu généralement, dans le contexte du *Code criminel*, sur le fondement de l'article 487 ou 487.01, ou de la *Loi sur la concurrence*, en vertu de l'article 15 ou 16. La délivrance d'un mandat de perquisition est un acte de nature judiciaire accompli par un juge de paix, généralement *ex parte* et à huis clos, en raison de la nature même de la procédure. Un mandat de perquisition donne l'autorisation à un agent de la paix ou à un agent de la puissance publique de fouiller un bâtiment ou un lieu pour y chercher quelque chose ou, encore, de fouiller un système informatique se trouvant dans un bâtiment ou un lieu précis, pour y trouver des informations qui serviront à prouver une infraction, et de saisir cette chose ou ces informations.

La décision de la Cour Suprême du Canada, dans l'affaire *Hunter c. Southam*, établit clairement qu'une perquisition sans mandat, de prime abord, va à l'encontre de l'article 8 de la *Charte canadienne des droits et libertés*. D'autre part, même lorsqu'une autorisation a été obtenue, celle-ci doit être conforme à la *Charte*. Deux critères ont été élaborés à cet égard. Premièrement, celui ou celle qui autorise la perquisition, qu'il s'agisse ou non d'un juge, doit être à même de juger de façon totalement neutre et impartiale des droits de chaque partie concernée, l'État et l'individu. Deuxièmement, celui ou celle qui souhaite obtenir une telle autorisation doit attester sous serment avoir des motifs raisonnables (et non pas uniquement des soupçons) le portant à croire qu'une infraction a été commise et que des preuves se trouvent sur les lieux où la perquisition doit être effectuée.