CAPACITÉ D'ACCÈS LÉGAL OU CAPACITÉ D'INTERCEPTION DES TÉLÉCOMMUNICATIONS?

Mémoire en réponse à la consultation sur l'accès légal menée par le gouvernement du Canada

Commission d'accès à l'information
Direction de l'analyse et de l'évaluation

Décembre 2002

Avant-Propos

Depuis le 11 septembre 2001, la lutte au terrorisme et à la criminalité a pris une importance que nous aurions eu peine à soupçonner auparavant. Battant le pas, les dirigeants des États-Unis exigent de leurs alliés la mise en place de mesures pour lutter contre les fléaux qui les accablent. Les pays interpellés proposent des réponses qu'ils pensent susceptibles de satisfaire aux demandes américaines.

La *Convention sur la cybercriminalité* est un traité dont les origines remontent à plusieurs années, bien avant les événements tragiques de 2001. Cette convention, sous l'égide du Conseil de l'Europe, visant à combattre le crime dans le monde virtuel fut l'objet de pas moins de 27 versions différentes. Elle propose des moyens de lutte contre le crime allant de l'interception des télécommunications à la conservation de certaines données sur les utilisateurs qui communiquent; ces mesures furent alors considérées par plusieurs défenseurs des droits des individus comme une fronde des plus liberticides.

C'est en novembre 2001, peu de temps après les attaques terroristes dirigées vers les États-Unis, que le Canada à l'instar d'une trentaine d'autres pays signa la *Convention sur la cybercriminalité*. Le gouvernement du Canada doit maintenant modifier sa législation afin de se conformer à cette convention. Par la suite, la ratification de ce traité confirmant l'engagement canadien à le respecter pourra avoir lieu. C'est dans ce contexte que le gouvernement canadien procède à une consultation sur ce qu'il a baptisé l'accès légal avant de présenter un projet de loi en ce sens.

L'accès légal permet aux agents d'application de la loi d'accéder aux données requises pour réaliser les enquêtes qu'ils mènent dans la lutte contre le crime. Selon le document de consultation du gouvernement fédéral, sa capacité d'accès légal est menacée par l'avènement de nouvelles technologies de communication. Du même souffle, il explique le désir du gouvernement de ratifier la *Convention sur la cybercriminalité*. Pour ce faire, il est proposé de modifier les lois existantes afin de rendre possible le recours à l'interception des télécommunications sur une base généralisée et de bâtir une infrastructure technologique qui permet l'atteinte de ce but.

La Commission d'accès à l'information (la Commission) a choisi de répondre à la consultation menée par le gouvernement du Canada parce qu'elle interpelle tous les citoyens du Québec. Le projet soumis à la consultation risque d'avoir des impacts négatifs sur les droits fondamentaux des Québécois, notamment sur leur droit à la vie privée. Beaucoup d'organisations publiques et privées du Québec sont aussi visées par les desseins d'Ottawa qui espère leur confier un rôle central dans l'interception des communications.

Accès Légal et interception des télécommunications

Né en 1748, Jeremy Bentham, un enfant prodige capable de lire le Latin à l'âge de trois ans devint plus tard avocat, comme l'avait décidé son père. Désillusionné par le droit, il passa le plus clair de sa vie à critiquer les lois existantes et à proposer des voies pour les améliorer. Bentham, devenu philosophe, étudia de multiples sujets allant de la religion, en passant par la pauvreté et les lois internationales jusqu'à la réforme des prisons. Aux environs de 1787, dans une série de lettres destinées à un de ses amis, il élabora un nouveau concept architectural qu'il appela *panopticon.* Panoptique signifie « qui permet de voir sans être vu ». L'architecture imaginée par Bentham permettait la construction d'établissements pénitentiaires et de prisons aménagés de telle sorte que le surveillant pouvait voir chaque détenu dans sa cellule, sans être vu lui-même. Le contrôle des prisonniers s'effectuait par la sensation qu'ils éprouvaient d'être constamment épiés par des yeux leur étant par ailleurs totalement invisibles. Les travaux de Bentham auraient peut-être eu moins d'impact n'eut été de Michel Foucault. Ce philosophe français s'intéressa au *panopticon* dans ses études sur le « pouvoir » permettant le contrôle des corps et des esprits des individus dans le but de les faire entrer dans un cadre commun[1]. Aujourd'hui, avec en toile de fond l'offre de nouvelles possibilités de surveillance propres au monde numérique et de contrôle du comportement des individus sur les réseaux de communication, plusieurs personnes croient reconnaître l'avènement d'un *néo-panopticon*, dont le regard embrasserait l'ensemble des communications faites par les citoyens.

En juin 2002, Pierre Mounier dans un article paru dans le magazine d'information Homo Numericus et intitulé « Surveiller et punir : le panoptique est dans la puce », écrit : « Le fantasme que Michel Foucault appelait *panoptique* il y a quelques décennies à propos des plans proposés au dix-huitième siècle par Jeremy Bentham pour une prison parfaite, a pourtant plus de chance d'être réalisé, dans la mesure où, dans un univers numérique, la dépendance de l'individu à la technologie est effectivement absolu. Il est dès lors possible de surveiller, au moyen d'appareils appropriés l'ensemble des communications sur un territoire donné, et même de les enregistrer et de les stocker pour une utilisation éventuelle future. ».

Des projets existent, auxquels participe le Canada, où il est possible de « voir sans être vu ». Pensons à *Echelon,* ce système de surveillance des communications dont l'existence, niée par les pays l'ayant mis au monde, fut prouvée par une enquête du Parlement européen. Le projet sur l'accès légal est de cette mouture ; dans celui-ci, le gouvernement nous informe du besoin de mettre à jour cette capacité afin notamment de se conformer aux exigences posées par la *Convention sur la cybercriminalité.* Or, cette convention soulève l'ire des groupes de défense de la liberté et des droits de la personne sur le continent européen, et même sur la scène internationale, qui la considèrent comme liberticide. Aujourd'hui le gouvernement du Canada nous propose par sa consultation de se prononcer sur les modalités lui permettant de se conformer à la convention européenne

[1] Surveiller et punir, naissance de la prison, Michel Foucault, Bibliothèque des histoires, nrf Éditions Gallimard (1975).

sur la cybercriminalité, sans toutefois que le fond, c'est-à-dire les exigences posées par le contenu de ce traité, ne soit expliqué et débattu.

Pour respecter les termes de la *Convention sur la cybercriminalité*, le gouvernement fédéral doit modifier les dispositions législatives existantes pour rendre l'interception des télécommunications légale et doit se donner le pouvoir d'exiger des fournisseurs de services en télécommunications qu'ils se dotent de moyens techniques permettant cette interception. Les technologies visées par ce projet sont celles permettant les communications sans fil et les communications avec fil, de même que celles à la base du fonctionnement des réseaux, notamment Internet.

La Commission appuie sans hésitation les efforts de lutte contre la criminalité sous toutes ses formes. Cependant, elle préconise pour ce faire le recours à des moyens qui permettent la préservation de l'ensemble de leurs droits fondamentaux et le strict respect de la vie privée des citoyens. C'est pourquoi la Commission entend commenter le projet soumis à la consultation en ayant comme souci de répondre aux questions suivantes :

- Le projet soumis pour consultation risque-t-il de porter atteinte à la vie privée des citoyens du Québec? Les droits fondamentaux garantis par les chartes de protection des droits et libertés sont-ils préservés?
- Le gouvernement du Canada maintient-il sa capacité d'accès légal, comme il le soutient, ou l'accroît-il?
- Le gouvernement du Canada met l'emphase sur les gestes à poser pour se conformer à la *Convention sur la cybercriminalité* alors que la vraie question est : le gouvernement doit-il ratifier cette convention, du moins sous sa forme actuelle?

Pour trouver réponse à ces questions ou, à tout le moins pour dégager des pistes de réflexion, la Commission commentera le projet du gouvernement fédéral en évaluant sa propension à répondre positivement à certains principes de protection de la vie privée. À la rigueur, d'autres interrogations pertinentes seront posées.

1- ÉRECTION D'UNE GIGANTESQUE INFRASTRUCTURE D'INTERCEPTION

Le gouvernement fédéral entend doter le Canada d'une imposante infrastructure d'interception des communications avec fil, sans fil et Internet. Celle-ci serait érigée sur la base d'exigences fonctionnelles spécifiant l'ensemble des détails techniques et des normes auxquels les fournisseurs devraient se conformer. Le tout serait scellé par voie réglementaire.

Chaque composante de cette toile d'interception reposerait chez chacun des fournisseurs de services qui existent au Canada. Un peu comme des terminaisons nerveuses réparties dans tous les recoins d'un corps vivant informent le cerveau auquel elles sont reliées,

chaque fournisseur réparti sur le territoire canadien ferait office de rapporteur aux autorités centrales.

Les fournisseurs seraient ainsi contraints, sous peine de sanctions, de se doter d'une capacité technique standardisée d'accès 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. Cette participation forcée serait combinée à l'obligation **d'identifier les utilisateurs** d'un service.

Cette contrainte d'interception et l'érection de la gigantesque infrastructure qui permettrait de s'y conformer vise vraisemblablement à répondre aux exigences posées par la *Convention sur la cybercriminalité*[2].

Situation actuelle

Selon le document de consultation, « 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 ».

Nous en comprenons donc, qu'actuellement les agents d'application de la loi utilisent leurs propres solutions et mécanismes d'interception lorsque requis. Cette capacité d'interception viserait alors un individu ou quelques individus à la fois.

L'infrastructure : une solution à la recherche d'un problème?

Que le gouvernement fédéral s'assure d'une capacité d'interception des communications est une chose qui dans certaines circonstances établies pourrait peut-être s'avérer légitime. Le document présenté pour consultation, n'établit pas qu'il soit impossible pour les organismes chargés de l'application de la loi de réaliser des interceptions dans le monde numérique lorsque requis. Nous convenons cependant de la possibilité dans certains cas, ou face à des technologies spécifiques, que les forces de l'ordre aient de la difficulté à procéder à des interceptions nécessaires. Malheureusement, le document soumis à notre examen est si peu loquace à cet égard, qu'il nous est impossible de confirmer cette hypothèse. Il faut cependant retenir que globalement , la **nécessité** même d'implanter une immense toile d'interception ne fait l'objet d'aucune démonstration convaincante. On semble plutôt rechercher plus de rapidité et moins de contraintes pour réaliser des interceptions, comme nous le verrons un peu plus loin dans ce texte. Or, en aucun cas cette recherche de performance ne devrait présider à l'adoption de mécanismes technologiques démesurés et grandement susceptibles de porter atteinte aux droits fondamentaux des citoyens.

[2] Voir Annexe 1 pour plus de détails.

Outre le fait que la mise en place d'une vaste infrastructure de surveillance généralisée n'ait été justifiée, le gouvernement fédéral doit aussi prendre en compte l'existence de nombreux risques que son implantation générerait.

Visa le noir tua le blanc

En créant une infrastructure d'interception le gouvernement met en place un gigantesque système de surveillance de l'ensemble des communications effectuées par les citoyens, par les associations, par les organismes, par les entreprises et par les divers paliers de gouvernements. Il est à mille lieues de viser uniquement les criminels ou les personnes soupçonnées de l'être. En fait, les criminels et les terroristes de ce monde, bien au fait de l'existence de cette surveillance n'hésiteront pas à emprunter ou à inventer d'autres modes de communication qui ne seront pas sous la férule des surveillants. À terme, n'y a-t-il pas un risque important que seuls les citoyens et les entités captives des modes de communication proposés sur le marché soient surveillés?

Fournisseurs de services ou agents de l'État?

Le gouvernement projette de faire des personnes morales et physiques qu'elle définit comme des fournisseurs de services, et le cas échéant de leurs employés ou de leurs collaborateurs , des « **agents de l'État** » et ce, par le truchement d'une réglementation [3]. Il est ici important de noter que le Canada considère comme des fournisseurs de services non seulement les associations, les entreprises et les organismes publics, mais aussi les personnes.

Le recours à un grand nombre d'*agents* multiplie les points de vulnérabilité de l'infrastructure car elle offre une multitude de portes d'entrées au système. Une fonction de contrôle et de surveillance des citoyens est dès lors confiée à une partie de la population dont le rôle initial est d'offrir des services de télécommunications, ce qui accroît les risques que l'information soit détournée de sa finalité initiale.

Sans démagogie, la Commission ne peut que poser la question suivante : Un système procurant une telle capacité d'interception des modes de communication les plus populaires, et obligeant la collaboration d'un grand nombre d'*agents,* ne pourrait-il pas pour certains rappeler la surveillance exercée par les régimes totalitaires?

L'infrastructure : un libre-service international?

Par le truchement de la *Convention sur la cybercriminalité*, le gouvernement fédéral s'engage à mettre à la disposition de plus d'une trentaine de pays signataires, la puissance de la capacité d'interception procurée par la mise en place de son infrastructure[4].

[3] Voir Annexe 2 pour plus de détails.
[4] Voir Annexe 1 pour plus de détails.

À titre d'exemple l'article 26 de la Convention concernant l'information spontanée autorise les pays signataires, même en l'absence de demande préalable, à communiquer à un autre pays des informations obtenues dans le cadre de ses propres enquêtes lorsqu'ils estiment que cela pourrait aider le destinataire.

Bien qu'il soit compréhensible que dans un monde virtuel, le crime ne se confine pas toujours à l'intérieur du tracé de nos frontières, il y a tout de même lieu de se parer contre les excès et la frivolité. Il existe en matière de protection de la vie privée un principe internationalement reconnu appelé finalité. Le principe de **finalité** exige que l'utilisation des données personnelles collectées ne serve qu'aux fins prévues. Une ouverture trop grande à l'égard de la communication par delà les frontières de données sensibles génère des risques d'abus dans l'utilisation, et de détournement de finalités par des pays tiers. Malgré tous les mécanismes mis en place pour contrer cette faiblesse, cette possibilité existera désormais.

Risques pour la vie privée

Le gouvernement en exigeant des fournisseurs de services[5] qu'ils mettent en place un mécanisme pour recueillir des données non nécessaires à leur activités commerciales, privées ou autres va à l'encontre du principe de **nécessité de la cueillette de renseignements**. En effet, un fournisseur ne doit recueillir que les seules données lui étant nécessaires pour rendre le service qu'une personne requiert. Ce principe est un pilier fondamental assurant la protection de la vie privée au même titre que la **finalité** déjà présentée ci avant. Par ailleurs, si l'État prétendait introduire ici une nouvelle finalité ce ne serait sûrement pas pour les besoins des fournisseurs de services.

Dans l'actuel projet, l'existence d'une infrastructure standardisée accroît les risques de détournement de finalité et d'utilisation abusive non seulement par les pays signataires du traité mais aussi par l'État, par les fournisseurs de services eux-mêmes et par des tiers qui poursuivent des buts illicites ou même dans certains cas politiques[6]. Une infrastructure, telle que celle proposée, exciterait sûrement la convoitise des éminences du crime organisé, de criminels et de terroristes, qui se gaussent des peines potentielles en cas de transgression des règles d'accès. La sécurisation de l'infrastructure demeure un défi colossal.

[5] Pour le gouvernement fédéral, 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 Canada. Dans le traité européen un fournisseur de service désigne toute **entité publique ou privée** qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique et toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

[6] Voir par exemple : Pierre Trudeau a insisté pour que la GRC espionne le Parti québécois, Dean Bibby, MesNouvelles.com, Presse Canadienne, Halifax, 22 octobre 2002.

L'infrastructure : un frein à l'innovation des technologies destinées à protéger la vie privée

Le projet qui nous est soumis exige des fournisseurs de services qu'ils incorporent aux nouveaux services qu'ils offriraient une capacité d'interception intrinsèque. Cette exigence risque d'empêcher le développement de nouveaux projets et de nouvelles technologies aptes à protéger la vie privée (exemple : Onion Router) ou offrant des capacités de communication anonyme (exemple : anonymizer). On peut même s'interroger à savoir si certaines des technologies de protection de la vie privée pourront encore exister. Par exemple, si un service d'émission de certificats permettant l'utilisation de clés de chiffrement nécessite le recours à un registre de validation en ligne, le promoteur de ce service sera-il inclus dans la définition de « fournisseur de services »? Devra-t-il alors offrir une capacité d'interception, annulant ainsi les effets du chiffrement?

Exemption

Le gouvernement fédéral prévoit l'exemption d'appliquer la capacité d'interception pour certains fournisseurs de services dans des situations particulières. Cette exigence est commandée par la *Convention sur la cybercriminalité*[7].

L'approche suggérée est que le Cabinet délègue son pouvoir d'exemption conjointement au Solliciteur général et au ministre de l'Industrie. Ces deux ministères élaboreraient des lignes directrices qui s'appliqueraient au traitement des demandes d'exemption.

Le document de consultation suggère une mécanique d'exemption sans spécifier les conditions qui la permettent; il y aurait pourtant lieu d'être clair à ce sujet. Concernant la mécanique proposée, elle comporte des dangers laissant dans les mains de ceux qui proposent l'interception le pouvoir d'exempter.

L'exemption signifie que si effectivement ce régime est mis en place, tous seront surveillés, sauf exception.

Mécanisme de conformité

Le gouvernement fédéral désire s'assurer, par des inspections et des analyses, que les fournisseurs de services respectent la loi. Ce mécanisme permettrait de se conformer aux exigences de la *Convention sur la cybercriminalité* qui va jusqu'à demander des sanctions pour les fournisseurs de services qui négligeraient de surveiller leurs employés, parce que ceux-ci pourraient omettre d'intégrer aux systèmes les mécanismes d'interception ou encore pourraient accéder et utiliser de manière abusive l'infrastructure d'interception. Dans certains cas les sanctions doivent être des *peines privatives de liberté*[8].

[7] Voir Annexe 1 pour plus de détails.
[8] Voir Annexe 1 pour plus de détails.

Le document fédéral s'interroge sur les types de pénalités à imposer alors qu'elles sont déjà en partie prévues dans la *Convention sur la cybercriminalité*. Ces mesures sont très sévères pour les fournisseurs de services qui ne prendraient pas au sérieux leur rôle « d'agents fédéraux ». Celles-ci les obligent à une surveillance et un contrôle serrés de leurs employés, ce qui pourrait inférer sur la vie privée de ces derniers. En fait, pour éviter les foudres des autorités, les fournisseurs n'hésiteront pas à implanter des mesures fortes de surveillance des employés même si celles-ci sont excessives.

C'est sans compter que le mécanisme de conformité obligera de recourir à des « vérificateurs » ou à des « auditeurs » qui auront probablement accès aux données interceptées, ne serait-ce que dans le but de s'assurer de l'effectivité du processus.

2- UTILISATION DE L'INFRASTRUCTURE : MODE D'EMPLOI

Dans le premier chapitre nous avons vu comment le gouvernement fédéral entend tisser sa toile d'interception. Cependant l'utilisation de l'infrastructure serait impensable à l'intérieur du cadre législatif actuel.[9] Pour cette raison, des assouplissements doivent nécessairement être apportés aux lois existantes. Une extrême prudence s'impose dans la modification de lois existantes et du *Code criminel*, ces derniers ayant été bâtis avec le souci de préserver les droits fondamentaux des personnes. Introduire plus de souplesse pour permettre de surveiller « sans être vu », avec des conditions d'exercice trop lâches, signifierait un renoncement à ces droits. La marge de manœuvre souhaitée par le gouvernement est introduite par la création de deux types principaux d'ordonnances et leur incorporation à la législation existante.

Les ordonnances

Le document de consultation présente deux grands types d'ordonnances : de production et de conservation.

Ordonnances de production

Le Canada semble vouloir répondre aux exigences de *la Convention sur la cybercriminalité*, en introduisant l'ordonnance de production[10].

Situation actuelle

Selon le document de consultation, les organismes d'application de la loi obtiennent un mandat de perquisition du tribunal lorsqu'ils désirent obtenir certaines informations. Deux critères existent pour qu'on recourt à un tel mandat :

[9] Voir Annexe 3 pour connaître les conditions d'interception actuelles.
[10] Voir Annexe 1 pour plus de détails.

- « 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 »;
- « 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 ».

Toujours selon le document de consultation, pour des raisons d'ordre pratique lorsqu'un mandat vise une société ou une banque, c'est souvent ces organismes qui produisent les documents en leur possession, sans qu'un agent n'effectue lui-même la perquisition.

La vie privée : une enfarge?

Une ordonnance de production exigerait d'un possesseur d'informations qu'il produise ou rende disponibles les documents à des agents responsables de l'application de la loi dans un délai précis. Ainsi plutôt qu'obtenir un mandat de perquisition, on demanderait au possesseur d'un document de faire le travail de la police ou d'un autre agent. Le document de consultation affirme qu'actuellement : « 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. ». Si c'est déjà la pratique avec le mandat de perquisition, pourquoi la changer? La réponse à cette question est peut-être dans la phrase suivante : « 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.** ».

Le document de consultation présente comme une enfarge le fait qu'aux termes du *Code criminel* un organisme d'application de la loi doit avoir des **motifs raisonnables de croire qu'une infraction a été commise ou sera commise** pour obtenir des documents ou des renseignements. Il se plaint que ceci **tient compte des intérêts relatifs à la vie privée.** On souhaite en conséquence qu'une ordonnance spécifique de production comporte un critère moins contraignant pour permettre la production de données relatives aux télécommunications. À cet égard le document de consultation dit : **« 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. ».**

À cette étape, nous constatons une banalisation des mécanismes visant à assurer la protection des droits fondamentaux et de ce qu'est un renseignement personnel. Cette surprenante façon de penser exprimée dans le document du gouvernement fédéral est lourde de conséquences et laisse supposer que l'ordonnance de production vise à amoindrir les droits fondamentaux des citoyens, principalement le droit à la vie privée. Le document va

jusqu'à prétendre que les critères de protection relatifs aux données concernant le trafic en temps réel devraient être les mêmes que ceux applicables aux enregistreurs de numéros de téléphone. Un numéro de téléphone révèle le nom de l'abonné, (sans savoir qui a utilisé la ligne) qui ou quelle entité fut contacté et ne dit rien sur les sujets de conversation. Ce n'est aucunement le cas avec les traces de navigation laissées par un internaute.

Les traces de navigation révèlent quel site a été visité, quelles pages contenant tel sujet furent consultées à telle heure et pour quelle durée. Plus simplement comparons la composition d'un numéro de téléphone et la navigation avec la visite à une bibliothèque publique. À ce moment, composer un numéro de téléphone équivaudrait à savoir que quelqu'un a visité une bibliothèque en particulier. Les données de trafic révèlent plus : chaque local visité dans la bibliothèque, à quelle heure et pour quelle durée, chaque livre ou périodique consulté ainsi que chaque page consultée, à quelle heure et pour quelle durée.

Comme si cela n'était pas assez, les ordonnances de production permettraient aussi d'obtenir des renseignements personnels (nom, adresse de facturation, numéro de téléphone, nom du fournisseur…) d'un individu « qui ne révèlent pas des détails intimes sur son mode de vie et ses choix personnels » selon les termes employés dans le document de consultation. On veut aussi obtenir ces renseignements « **pour des raisons non reliées à une enquête ou parce qu'il s'agit d'un début d'enquête** ». Actuellement, en conformité avec la *Loi sur la protection des renseignements personnels et les documents électroniques* (Canada) ces renseignements ne peuvent être communiqués sans la connaissance et le consentement de l'individu visé à un organisme qui doit faire la preuve légale de son droit d'obtenir ces renseignements. Le document de consultation se plaint de ces exigences ayant pour but de protéger la vie privée en ces termes : « 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 des renseignements relatifs au client ou à l'abonné en l'absence d'une ordonnance du tribunal à cette fin. ».

La Commission ne peut que dénoncer la banalisation et les affirmations sans fondement faites dans le document de consultation à l'égard de certains types de renseignements personnels et concernant les principes de protection de la vie privée. Il est ironique de penser qu'au moment même où la main droite du gouvernement tente d'offrir des solutions aux citoyens pour les rassurer sur la protection de leur vie privée dans la prestation de services électroniques (e- gouvernement), sa main gauche tente d'amoindrir la portée des protections qui lui sont offertes.

En fonction des informations reçues, **le gouvernement fédéral n'a pas démontré la nécessité de recourir à un mécanisme d'ordonnance de production.** Les circonstances dans lesquelles une ordonnance pourrait être émise laissent craindre un amoindrissement de la protection de la vie privée et d'autres droits fondamentaux.

Ordonnances de conservation

Selon le document de consultation, ce mécanisme procédural n'existe pas actuellement en droit canadien. Le but recherché serait donc uniquement de se plier aux exigences de la *Convention sur la cybercriminalité*[11]. Ce type d'ordonnance exige d'un fournisseur de services de stocker et de conserver toutes les données existantes qui se rapportent à une transaction ou à un client spécifique. Le gouvernement propose aussi qu'un « 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 » dans des circonstances extraordinaires.

Malgré l'existence de l'ordonnance de conservation, le document de consultation nous informe que **« le stockage est une exigence générale selon laquelle les fournisseurs de services pourraient être tenus de *recueillir et de stocker certaines données concernant tous leurs abonnés*. ».** Cette exigence de stockage pour les besoins non basés sur des assises factuelles et non clairement définie laisse craindre **un fichage généralisé d'une grande partie de la population.**

Après examen des informations contenues au document de consultation, la Commission constate que le gouvernement du Canada n'a pas démontré le besoin d'instaurer un tel mécanisme sur son territoire.

Interception du courrier électronique

Dans le document de consultation du fédéral, il est supposé que : « …**lorsqu'une communication est consignée par écrit, il ne s'agit plus réellement d'une communication privée**[12] aux fins des dispositions relatives à l'interception des communications en vertu du *Code criminel*. ». « 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.** ». Cependant, selon le document, un courrier en transit chez un tiers ou en attente de livraison pourrait être privé ; pour le gouvernement fédéral c'est déjà trop! Il espère ainsi modifier les lois et le *Code criminel* afin de pouvoir intercepter en tous lieux le courrier électronique. Une fois de plus le gouvernement du Canada semble répondre par l'interception du courrier aux impératifs posés par la *Convention sur la cybercriminalité*[13].

[11] Voir l'Annexe 1 pour plus de détails.
[12] Le document nous informe aussi que : « Toutefois, dans certaines affaires relatives au courrier électronique au Canada, les tribunaux ont jugé qu'il s'agissait de *communications privées* ».
[13] Voir Annexe 1 pour plus de détails.

La Commission est d'avis que le contenu d'un courrier électronique constitue en tout temps une communication privée et que son interception de façon généralisée bafoue le droit à la vie privée des citoyens. Les criminels se sachant surveillés utiliseront d'autres modes de communication et en bout de piste ce sont les citoyens honnêtes qui feront l'objet d'une surveillance et d'un fichage injustifiés de leurs communications.
La Commission demande au gouvernement de cibler la criminalité plutôt que des citoyens honnêtes. La proposition d'intercepter le courrier électronique ne fait que renforcer le rôle « d'agents de l'État » que le gouvernement désire confier aux fournisseurs de services.

3- AUTRES MOYENS PERMETTANT DE RECUEILLIR DES RENSEIGNEMENTS SUR LES ABONNÉS ET LES FOURNISSEURS

Création d'une base de données nationale

Le document de consultation se plaint que depuis la déréglementation du marché des télécommunications, les organismes d'application de la loi « doivent consacrer beaucoup de temps à identifier le fournisseur de services locaux ». De plus, pour obtenir un renseignement sur un abonné un tel organisme doit « contacter directement chaque fournisseur local, ce qui constitue un processus long et coûteux ».

Pour contrer ce « problème », le document propose la création d'une base de données nationale contenant le nom des fournisseurs de services et leur adresse ainsi que le nom et l'adresse de tous les clients de ce fournisseur. Les informations contenues dans cette base de données sont jugées dans le document de consultation **non confidentielles**. Cette banalisation laisse craindre que ce dépôt de données nominatives soit accessible à tous, particulièrement aux autres pays signataires de la convention européenne. Le gouvernement veut aussi recourir à des sources de renseignements existantes comme les données du service 911 et des répertoires téléphoniques privés. En fait, la création de la base de données centrale et l'accès à des dépôts de données existants semblent uniquement répondre aux exigences d'accès transfrontières imposées par la *Convention sur la cybercriminalité*[14].

La Commission est d'avis qu'il est impossible de créer une mégabanque comme celle projetée dans le document de consultation tout en respectant la vie privée des citoyens. Elle déplore aussi l'intention avouée de détourner la finalité d'autres dépôts de données comme les services d'urgence 911. Le gouvernement n'a pas démontré la nécessité de recourir à de tels moyens et ne doit surtout pas créer une telle banque dans le seul but d'en rendre le contenu disponible à d'autres pays.

Par surcroît, la Commission estime que les données confiées par les citoyens aux fournisseurs le sont dans le but de recevoir un service et servent notamment à établir la facturation. Les verser dans un répertoire national et accessible largement constituerait un détournement de finalité.

[14] Voir l'Annexe 1 pour plus de détails.

Cueillette de données :

Le document de consultation se plaint aussi que dans certains cas « se pose 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 ». Pour contrer cette pratique, le gouvernement aimerait que les fournisseurs de services de télécommunications soient tenus de recueillir de tels renseignements et d'en assurer la précision, l'intégralité et la fiabilité.

La Commission considère que les fournisseurs de services qui ne recueillent pas ces renseignements n'ont aucune nécessité de le faire et qu'ils ne doivent pas devenir des « agents de collecte » de renseignements au bénéfice de l'État.

En définitive :

Le document de consultation présenté est truffé de non-dits et d'imprécisions. L'accent est mis sur le mécanisme alors que les enjeux en matière de droits fondamentaux se situent sur le fond. Aucune démonstration convaincante de la nécessité d'instaurer un système de surveillance permettant de « surveiller sans être vu » et du fichage de l'ensemble des citoyens n'est faite. Le contenu de la *Convention sur la cybercriminalité* n'est ni présenté, ni expliqué alors que la plupart des modifications légales et des pouvoirs demandés le seraient vraisemblablement pour répondre à celle-ci. C'est sans compter que le projet fait des fournisseurs de services des « agents de l'État » qui prêteront leurs yeux au gouvernement fédéral. Si ce projet n'est pas un *néo-panopticon*, il en possède à tout le moins quelques attributs.

Le gouvernement du Canada veut s'accorder une grande marge de manœuvre dans l'utilisation de l'infrastructure d'interception qu'il espère ériger. Cette marge risque d'amoindrir les protections offertes aux citoyens comme la présomption d'innocence, le droit au secret, le droit à l'anonymat et le droit du respect de la vie privée. Elle risque aussi d'abolir la nécessaire séparation qui doit exister entre l'administration de la justice et les agents d'application de la loi et qui garantit l'équilibre des pouvoirs. Elle permet aux « polices » d'une trentaine d'États signataires de la convention un accès facilité à des données sensibles. Qui contrôlera effectivement l'infrastructure géante constituée par la trentaine d'infrastructures nationales? Puisqu'il s'agit en fait d'une infrastructure commune à plusieurs pays, à l'image du système Échelon, qui surveillera les surveillants? Échapperont-ils à tout contrôle international? La police et les agents seront sous le contrôle de qui et rendront des comptes à qui?

Le désir de ratifier un traité international ne saurait aucunement justifier le recours à un mécanisme de surveillance généralisée. Seul un besoin impérieux de sécurité serait susceptible de répondre à cette justification et encore faudrait-il que le moyen choisi soit proportionnel aux menaces existant réellement. Or, le document de consultation n'établit pas l'existence de telles menaces.

Commission d'accès à l'information
Mémoire en réponse à la consultation sur l'Accès Légal
Décembre 2002

Annexe 1 –Liens entre la proposition fédérale et la Convention sur la cybercriminalité[15]

Sujet : Capacité d'interception
Situation dans le texte : Page 4, note de bas de page 3**;**
Référence dans la Convention :

Chapitre II – Mesures à prendre au niveau national
Section 2 – Droit procédural
Titre 5 – Collecte en temps réel de données informatiques
Article 20 – Collecte en temps réel des données relatives au trafic
Article 21 - Interception de données relatives au contenu

Sujet : Coopération internationale
Situation dans le texte : Page 5, note de bas de page 5.
Référence dans la Convention :

Chapitre III – Coopération internationale
Section 1 –Principes généraux
Titre 1 – Principes généraux relatifs à la coopération internationale
Titre 2 – Principes relatifs à l'extradition
Titre 3 – Principes généraux relatifs à l'entraide

Sujet : Exemption
Situation dans le texte : Page 6, note de bas de page 7.
Référence dans la Convention :
Chapitre II – Mesures à prendre au niveau national
Section 2 – Droit procédural
Titre 1 – Dispositions communes
Article 14 – Portée d'application des mesures du droit de procédure (3.b)

Sujet : Mécanisme de conformité et sanctions.
Situation dans le texte : Page 7, note de bas de page 8.
Référence dans la Convention :
Chapitre II – Mesures à prendre au niveau national
Section 1- Droit pénal matériel
Article 13 – Sanctions et mesures

[15] Ces liens avec la Convention sur la cybercriminalité sont présentés à titre indicatif. Ils n'ont ni la prétention d'être complets et rigoureusement exacts.

Sujet : Ordonnance de production.
Situation dans le texte : Page 8, note de bas de page 9.
Référence dans la Convention :
Chapitre II – Mesures à prendre au niveau national
Section 2 – Droit procédural
Titre 3 – Injonction de produire
Article 18 – Injonction de produire
Article 19 – Perquisition et saisie de données informatiques stockées

---

Sujet : Ordonnance de conservation**.**
Situation dans le texte : Page 9, note de bas de page 10.
Référence dans la Convention :
Chapitre 2 – Mesures à prendre au niveau national
Section 2 – Droit procédural
Titre 2 – Conservation rapide de données informatiques stockées
Article 16 - Conservation rapide de données informatiques
Stockées
Article 17 – Conservation et divulgation rapides de données relatives au trafic

---

Sujet : Interception du courrier électronique.
Situation dans le texte : Page 10 , note de bas de page 11.
Référence dans la Convention :
Chapitre II – Mesures à prendre au niveau national
Section II – Droit procédural
Titre 5 – Collecte en temps réel de données informatiques
Article 21 – Interception de données relatives au contenu

Sujet : Création d'une base de données nationale
Situation dans le texte : Page 11, note de bas de page 12.
Référence dans la Convention :
Chapitre III – Coopération internationale
Section 2 – Dispositions spécifiques
Titre 2 – Entraide concernant les pouvoirs d'investigation
Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

---

Commission d'accès à l'information
Mémoire en réponse à la consultation sur l'Accès Légal
Décembre 2002

Annexe 2 - Contenu de la réglementation imposée aux fournisseurs de services

- Normes et détails techniques de l'infrastructure;
- Équipement à installer, annexer ou lier;
- Exigences de capacité du nombre maximal d'interceptions simultanées;
- Modalités et conditions relatives à la sécurité d'interception;
- Modalités et conditions relatives à la transmission des résultats des interceptions;
- La compétence, la fiabilité et la mise en place du personnel.

Commission d'accès à l'information
Mémoire en réponse à la consultation sur l'Accès Légal
Décembre 2002

Annexe 3 – Conditions actuelles pour réaliser une interception (tiré du document de consultation)

- 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.