LIGUE DES DROITS ET LIBERTÉS

Mémoire sur l'« accès légal » en réponse à la consultation menée par le Ministère de la Justice du Canada

Décembre 2002

Ligue des droits et libertés

65, rue de Castelnau Ouest, bureau 301 • Montréal (Québec) H2R 2W3
Téléphone : (514) 849-7717 • Télécopieur : (514) 849-6717 • Courriel : ldl@biz.videotron.ca

La *Ligue des droits et libertés* est un organisme à but non lucratif, indépendant et non-partisan fondé en 1963. Les objectifs poursuivis par la Ligue sont la défense et la promotion des droits reconnus dans la *Charte internationale des droits de l'homme*., dont elle soutient l'universalité et l'indivisibilité La *Ligue des droits et libertés* est membre de la *Fédération internationale des ligues des droits de l'homme.* Elle est une des plus anciennes organisations de droits des Amériques.

Introduction

Le ministère de la Justice du Canada publiait, le 25 août 2002, un document de consultation intitulé « Accès légal ». Ce document annonce les grands principes d'une future législation permettant d'une part d'augmenter les capacités de surveillance électronique en les adaptant aux **technologies actuelles et futures** liées aux systèmes informatiques et, d'autre part, d'obliger les fournisseurs de ce type de communications (dont les « serveurs »), de stocker et conserver des données afin de les remettre éventuellement aux personnes chargées de l'application de la loi, incluant les fonctionnaires de certains ministères, dont le ministère du Revenu. Cette législation permettra d'intercepter le courrier électronique, d'obtenir toutes les données (acheminement, contenu) sur un abonné ou un fournisseur.

L'enfer est pavé de bonnes intentions. Le document de consultation s'appuie sur des objectifs à première vue louables et légitimes : protection de la confidentialité et de la propriété intellectuelle, lutte contre la pornographie infantile, lutte contre le terrorisme et contre les virus informatiques. Toutefois le projet a des conséquences dépassant de loin la simple répression de ces crimes particuliers et risque de nous faire basculer dans un monde, où nos courriers électroniques, nos consultations et visites sur Internet, où nos moindres gestes pourront être épiés de façon continue, où nous serons comme des microbes sous le microscope.Ce projet de législation s'appuie sur la volonté de se conformer à la Convention sur la cybercriminalité que le Canada a signée le 12 août 2002, sans l'avoir encore ratifiée ni avoir déposé de réserve ou dénonciation. Le document de consultation indique que : « *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…* »[1].

Pouvoir d'interception exorbitant du droit commun

Normalement, pour pouvoir procéder à l'écoute électronique de conversations privées, il faut obtenir une autorisation judiciaire après avoir démontré que l'on a des motifs raisonnables et probables de croire à la commission d'une infraction. Le gouvernement souhaite un « *critère moins contraignant que les motifs raisonnables* ».

De plus le gouvernement voudrait utiliser certains de ces pouvoirs de surveillance lors de la phase du « *début d'enquête* », et ce, sans aucune autorisation judiciaire.

[1] *Accès légal*, document de consultation, 25 août 2002, p. 6.

Comme le signale le Commissaire à la protection de la vie privée du Canada, M. George Radwanski : « Les agents de l'État du Canada ne peuvent demander à la Société canadienne des postes de photocopier l'adresse figurant sur chaque enveloppe que nous expédions, ni aux librairies de conserver un registre de tous les livres que nous achetons, et encore moins de toutes les pages de toutes les revues que nous feuilletons. Il n'y a aucune raison de pouvoir exercer de tels pouvoirs en ce qui concerne tous les courriels que quelqu'un envoie ou tous les sites Web qu'il consulte. » [2]

À l'instar de M. George Radwanski, nous croyons que la démonstration de la nécessité d'une telle intrusion dans la vie privée des Canadiennes et des Canadiens n'a pas été faite.

Les dispositions existantes du Code criminel permettent déjà l'interception électronique ainsi qu'une procédure permettant d'obtenir une ordonnance d'assistance du fournisseur de service (articles 183 et al et 487 et particulièrement 487.02 C. cr.).

En fait, le gouvernement canadien désire abaisser les exigences requises, qui sont des protections procédurales de la vie privée, pour opérer une interception ou surveillance électronique.

Le processus de consultation

Une équipe formée de représentants de différents ministères a effectué une « tournée de consultation » dans trois villes (Ottawa, Montréal, Vancouver). Lors de la rencontre de Montréal, le caractère vague des réponses des fonctionnaires était aussi inquiétant que le projet de législation. Le document de consultation invitait les organisations et individus à présenter leurs observations d'ici le 15 novembre 2002, cette date a été reportée par la suite au 16 décembre.

Le *Rapport explicatif* de la *Convention sur la cybercriminalité* (sur laquelle s'appuie le projet de législation) indique qu'une 1ère version du texte de la convention a été rendue publique en avril 2000 afin de permettre aux États de consulter la société civile [3] et ceci avant la signature du traité. Le Canada a signé la Convention le 12 août 2002[4] mais selon le document de consultation, il appert qu'il avait déjà commencé un examen global des lois depuis octobre 2000[5]. Le projet annoncé est sans précédent et aura un impact important sur toute la société, son fonctionnement et l'ensemble des relations entre ses différentes composantes. Les organisations de la société civile ne font que commencer à prendre connaissance de ce projet et sont peu conscientes des impacts. Par ailleurs, il est étrange que le comité de consultation du ministère de la Justice n'ait visité que trois villes et n'ait pas cru bon d'effectuer un arrêt à Toronto. La *Ligue des droits et libertés* ne peut que constater l'absence d'un véritable débat public sur la question de la surveillance de données informatiques rendu pourtant nécessaire à cause des impacts importants que cette surveillance aura sur la vie privée.

---

[2] Extrait de la lettre que le Commissaire à la protection de la vie privée du Canada, George Radwanski, a envoyé au ministre de la Justice et Procureur général du Canada, Monsieur Martin Cauchon, à Monsieur Wayne Easter, Solliciteur général du Canada, ainsi qu'à l'honorable Allan Rock, ministre de l'Industrie, au sujet des propositions relatives à « l'accès légal », 25 novembre 2002.

[3] *Rapport explicatif*, adopté le 8 novembre 2001, paragraphe 14.

[4] *Accès légal*, précité, p. 7.

[5] *Accès légal*, précité, p. 8.

Accumulation de pouvoirs de contrôle et de surveillance

Depuis un an, la population canadienne ne cesse d'être assujettie à un nombre toujours croissant de structures de surveillance policière. Une juste analyse de la Convention et du projet de législation amène à prendre en compte cette nouvelle réalité. Citons-en quelques-unes, certaines déjà en vigueur, et d'autres encore à l'état de projet :

a) Les nouvelles dispositions relatives au terrorisme adoptées avec le projet de loi C-36, et particulièrement :

- La définition large d'activité terroriste incluant des actes contre la « sécurité nationale » et contre la « sécurité économique »;
- Les vastes pouvoirs conférés aux forces de l'ordre, leur permettant d'interroger, surveiller, détenir (pour fins d'interrogatoire) et ficher des personnes sur lesquelles ne pèsent que de simples soupçons d' « activités terroristes »;
- L'instauration du secret dans les procédures relatives aux procès pour terrorisme;
- Les nouvelles dispositions portant sur la sécurité nationale;
- L'allégement des conditions permettant l'écoute électronique;
- L'élargissement des pouvoirs du CST (Centre de la sécurité de télécommunications), organisme dépendant du ministère de la Défense.

b) La mise en vigueur, en février 2002, de l'article 25.1 du Code criminel (projet de loi C-24), accordant aux policiers l'immunité pour la majorité des infractions criminelles, si elles sont commises dans le cadre d'une enquête;

c) L'instauration d'un mégafichier portant sur les personnes voyageant par avion à l'extérieur du pays. Le ministère du Revenu a déjà annoncé que d'ici 2004, ce sont tous les voyageurs qui utilisent le transport par train, autobus et bateau qui seront progressivement fichés;

d) Le projet de loi C-17 actuellement en voie d'adoption, octroyant à la GRC, et au SCRS, un accès sans restriction aux renseignements que les sociétés aériennes obtiennent sur leurs passagers. De plus la GRC serait habilitée à utiliser ces renseignements pour repérer toute personne à l'égard de laquelle un mandat aurait été délivré même pour une infraction pénale qui serait sans aucun rapport avec le terrorisme, la sécurité des transports ou la sécurité nationale;

e) Le projet d'une carte d'identité canadienne, qui comporterait cette fois des données biométriques, comme les empreintes digitales ou l'image de l'iris;

f) L'annonce en octobre 2002 de la création d'une autre base de données qui, elle, contiendra les photos numérisées des 10 millions de Canadiens et de Canadiennes qui détiennent un passeport.

Danger de la mise en place d'une base de données

Les capacités de surveillance pourraient être multipliées par l'accumulation et le couplage de données entre les différents fichiers et informations obtenues par les services policiers et les ministères. Le risque est élevé que les informations recueillies sur des citoyens innocents lors d'opération de surveillance électroniques soient un jour ou l'autre stockées dans des bases de données pour utilisation future.

Le *Commissaire à la protection de la vie privée du Canada* souligne qu'une politique d'ordonnance générale de rétention de données relatives aux communications par Internet et par téléphone cellulaire « serait une invasion impardonnable de la vie privée (…) »[6].

Tant le document de consultation que la *Convention sur la cybercriminalité* suggèrent la possibilité d'accumulations des données concernant tous les abonnés d'un fournisseur. Et, toujours grâce à la technologie informatique, il ne serait pas si difficile d'évoluer vers un fichier central où s'accumuleraient les données exigées des divers fournisseurs de services. D'autre part, l'inquiétude vient de ce qu'on sait déjà de la façon dont les corps policiers et les services de renseignement utilisent ces nouvelles sources d'informations: couplages de fichiers, rapprochement d'informations, « balayage » à l'aide de « profils ».

Les policiers recourent au couplage des informations, en rapprochant les informations fournies par diverses bases de données. De plus, ils interrogent les bases de données en leur appliquant divers « profils », dessinés à partir de caractéristiques personnelles, de comportements ou d'habitudes. C'est ainsi d'ailleurs qu'on interroge le fichier, récemment mis en place, sur les déplacements internationaux des voyageurs. Et c'est la façon de travailler également au CANAFE (Centre d'analyse des opérations et déclarations financières du Canada). La pression sera forte pour qu'il devienne de plus en plus simple d'avoir un accès rapide aux données de cette multitude de fichiers tous plus intéressants les uns que les autres, notamment pour les organismes de contrôle et de surveillance. Et la suggestion de l'*Association canadienne des chefs de police* de créer une base de données nationale des noms, adresses et numéros de téléphone de tous les abonnés canadiens, si elle était retenue, pourrait n'être que le premier pas vers une grande base d'informations qu'on ne cesserait de vouloir enrichir.

La confection de mégafichiers (dont celui sur les personnes voyageant par avion), représente un risque supplémentaire de violation des droits et liberté. **L'accumulation et le couplage** de données, qui semblent de prime abord de peu d'importance et sans conséquence, comme les données de trafic, permettraient aux autorités de surveiller le mode de vie des citoyens. Ceci est une illustration des dangers liés au stockage infini d'informations rendu possible grâce à l'informatique et au recoupement de telles données : l'impact de ces technologies a un effet sans précédent sur les capacités de surveillance. Que dirions-nous si les agents de l'État pouvaient ainsi, subrepticement, suivre et surveiller les citoyens dans leurs allées et venues et ficher leurs déplacements quotidiens?

Interception limitée aux infractions graves ?

[6] Lettre du 25 novembre 2002 du *Commissaire à la vie privée du Canada*, précité.

L'article 21 de la Convention dispose expressément que les Parties ne sont tenues d'instaurer cette mesure qu'*en relation avec de graves infractions à définir dans le droit interne.*

Dans son introduction, le document de consultation prétend que « *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* »[7]. Le document de consultation indique que l'interception ne pourrait s'effectuer que si l'infraction présumée possède un *caractère suffisamment grave pour justifier une telle demande*[8].

Pourtant, les règles actuelles d'interception du Code criminel auxquelles le document se rapporte vont bien plus loin que la répression d'infractions graves, tel le meurtre, la trahison, la piraterie, l'homicide.

L'interception est aussi possible dans le cas des infractions répondant à la définition « d'infraction de terrorisme » dont le caractère excessif a été publiquement dénoncé lors de l'adoption du projet de loi C-36. Les dispositions actuelles réfèrent aussi à plus de 115 diverses infractions, incluant des infractions hybrides (poursuivables soit comme infraction sommaire, soit comme acte criminel) comme le méfait, le vol, les menaces, la possession ou la vente de produits du tabac ou d'alcool (*Loi sur l'accise*), certains articles de la *Loi sur les douanes* etc. On est loin d'une mesure limitée aux infractions graves.

La prétendue faible attente de vie privée

Dans son document de consultation, le gouvernement fédéral confère aux données recueillies par la saisie d'enregistrement de numéros de téléphone les mêmes impacts qu'aurait la saisie de « données de trafic ». Tenant compte du développement technologique en informatique et de la somme d'informations pouvant être recueillie avec les « données de trafic », la saisie de ces données ne peut être considérée équivalente à celle d'enregistreurs de numéros de téléphone. Les données de trafic permettent en effet de dévoiler dans le détail le mode de vie d'un citoyen. Par conséquent, la saisie des « données de trafic » devrait être soumise à des exigences et conditions similaires à celle des données de contenu.

Le document de consultation révèle l'intention du gouvernement **d'assouplir les exigences actuelles de surveillance électronique.** Alors que l'accès aux « données de trafic » constitue une véritable intrusion dans la vie privée, l'on cherche plutôt avec le projet « Accès légal » à définir des critères moins contraignants d'interception et de saisie. Le document de consultation soutient que les visites faites par chacun sur Internet n'appartiennent pas à la vie privée, ou si peu. De même, l'expectative de vie privée des citoyens serait moindre pour une communication électronique que pour une communication sur papier ou une conversation téléphonique. Pourtant, la quantité d'informations pouvant être communiquée lors d'une seule transmission par Internet,

[7] *Accès légal*, précité, p. 4.
[8] *Accès légal*, précité, p. 24.

en quelques secondes, est sans commune mesure avec une conversation téléphonique ou une lettre.

Excepté quelques mentions générales le document fait bien peu de cas des droits et libertés garantis par la *Charte canadienne des droits et libertés.* Le document insiste par ailleurs largement sur les principes de l'arrêt *Plant*[9] de la Cour suprême afin de justifier l'absence d'expectative de vie privée des « données de trafic ». Pourtant il n'y a aucune commune mesure entre les relevés de compteurs d'électricité disponibles à tout citoyen sur demande et les « données de trafic », *a priori* confidentielles, puisqu'elles dévoilent effectivement les habitudes de vie d'un individu[10]. Si le gouvernement entendait réellement garantir le respect de tous les droits fondamentaux inscrits dans la *Charte*, n'aurait-il pas dû éprouver le besoin de limiter davantage et d'encadrer très strictement le recours à ces pouvoirs de surveillance électronique?

Considérant que l'impact sur la vie privée de l'interception de données informatiques est encore plus grand que l'écoute téléphonique, les procédures et conditions pour l'obtention d'une autorisation devraient être à tout le moins les mêmes, sinon plus élevées, que les règles actuelles d'interception.

La *Convention sur la cybercriminalité*

La *Convention sur la cybercriminalité* a été élaborée par le *Conseil de l'Europe* avec la participation active de l'Afrique-du-Sud, du Canada, des États-Unis et du Japon. Selon certains, les négociations entre les États étaient vouées à l'impasse jusqu'aux événements du 11 septembre 2001. Le texte définitif a été adopté à Budapest, le 23 novembre 2001. Le 7 novembre 2002 était adopté un protocole additionnel portant sur *l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.*

La portée de la Convention dépasse de loin la répression de l'utilisation du courriel à des fins de propagation de virus, viol de confidentialité, vol de logiciel, pornographie infantile, lutte au terrorisme ou propagation de la haine raciale. La convention donne une définition large et englobante de l'utilisation de données informatiques. Les auteurs du *Rapport explicatif* de la *Convention sur la cybercriminalité* soulignent que :

> *Alors qu'initialement, seuls certains secteurs de la société avaient rationalisé leurs méthodes de travail en s'appuyant sur les technologies de l'information, il ne reste pour ainsi dire plus aucun secteur qu'elles n'aient marqué de leur empreinte. Les technologies de l'information se sont insinuées, d'une manière ou d'une autre, dans tous les aspects des activités humaines.*[11]

Par ailleurs, la Convention ne limite pas la surveillance, la saisie de données informatiques, de même que les obligations d'entraide entre États signataires, aux infractions pénales liées à des systèmes et des données informatiques mais aussi <u>*à la collecte de preuves sous forme*</u>

[9] *R.* c *Plant*, [1993] 3 R.C.S. 281
[10] Lire l'*Opinion de l'honorable Juge à la Cour suprême Gérard V. La Forest* sur le dossier du passager de l'ADRC (le mégafichier sur les voyageurs), lettre à M. George Radwanski, 19 novembre 2002
[11] *Rapport explicatif*, précité, paragraphe 1.

électronique se rapportant à une infraction pénale. Autrement dit, la Convention, tout comme le projet de législation du Canada, ne vise pas simplement la répression de crime commis par le biais de système informatique mais aussi l'utilisation, par les personnes chargées de l'application de la loi, des systèmes informatiques à des fins générales de surveillance et d'enquête.

L'entraide entre les États

La Convention à laquelle réfère le projet, soulève la question des informations recueillies et transmises à un autre État pour des motifs qui dépassent les enquêtes de polices usuelles. Ces motifs, souvent nébuleux, de relations internationales, élément indissociable du concept de *sécurité nationale*, permettent la surveillance de citoyens canadiens n'ayant rien à se reprocher afin de permettre à des organismes de surveillance étrangers de parfaire leurs banques d'informations. Ces échanges pourraient permettre à des organismes policiers étrangers, ou autres agents d'État, de faire ce qu'ils n'auraient pas le droit d'effectuer eux-mêmes, c'est-à-dire recueillir de l'information par le biais d'autres corps de surveillance, afin de parfaire leurs enquêtes. Les garanties procédurales de protection des droits de la personne varient effectivement d'un pays à l'autre.

La règle de la double incrimination et ses limites

Qu'arrivera-t-il quand un pays signataire demandera des informations sur un crime qui n'en serait pas un au Canada?

Les États signataires peuvent, **s'ils le signifient clairement** (y compris par une réserve à la Convention) appliquer la ***règle de la double incrimination***. Cette règle permet à un État signataire de refuser d'apporter assistance si l'infraction pour laquelle l'État requérant réclame l'assistance n'existe pas dans l'État requis (celui à qui l'on demande assistance)[12]. Toutefois cette exigence pourrait atteindre rapidement ses limites, ainsi que le *Rapport explicatif* l'indique[13]:

> *…cette condition sera considérée comme satisfaite si le comportement constituant l'infraction en relation avec laquelle l'entraide est requise est également qualifiée d'infraction pénale par le droit interne de la Partie requise, même si ledit droit interne classe l'infraction dans une catégorie d'infractions différente ou la désigne en utilisant une terminologie différente.*

Citons deux exemples :

- La pornographie infantile : il n'est pas certain que la définition de ce crime par les pays signataires (l'Albanie et la Croatie étant les deux premiers États à y avoir adhéré) soit la même que celle donnée par la Cour suprême dans l'arrêt *Sharp* (jurisprudence portant sur les limites de l'infraction : dessins et photos de famille, œuvre artistique, etc.). En Arabie Saoudite, l'on interdit la retransmission des matchs de football à partir de certains pays parce

[12] *Convention sur la cybercriminalité*, voir la définition au paragraphe 5 de l'article 25.
[13] *Rapport explicatif*, précité, paragraphe 259.

que l'on voyait, parfois, les bras dénudés de jeunes filles dans les tribunes[14]. Plus près de nous, une loi fédérale des États-Unis a été invalidée en avril 2002 à cause de sa portée trop large (*Ashcroft* v. *Free Speech Coalition*, [2002] SCT-QL 69, No 00-795), la Cour suprême des États-Unis jugeant que cette disposition rendrait illégale la diffusion de *Roméo et Juliette*.

- Les crimes racistes et xénophobes : en France, la *Loi Gayssot* criminalise le négationnisme (nier l'existence des camps de la mort nazi ou du génocide Rwandais) alors qu'au Canada, la Cour suprême a invalidé des dispositions similaires du Code criminel (soit la prohibition de publier des faussetés, l'affaire *Zundel*[15]), tout en prohibant la propagande haineuse (l'affaire *Keegstra*[16]).

Serait-il suffisant que le Canada réprime, par exemple, la pornographie infantile, même si la portée de l'infraction est différente de celle de l'État requérant, pour qu'il soit tenu d'apporter son assistance à un État désirant réprimer des actes qui ne sont pas des crimes au Canada?

La ratification de la Convention

Le Canada doit-il ratifier la Convention ? La *Ligue des droits et libertés* croit qu'il est trop tôt pour prendre position sur la nécessité, par le Canada, de ratifier ou non la *Convention sur la cybercriminalité*, sans qu'un véritable débat public soit tenu à ce sujet. Des questions devront être posées et éclaircies quant aux impacts et aux enjeux de cette convention.

Ne serait-il pas préférable que le Canada vérifie d'abord si la législation actuelle répond aux grands principes mis de l'avant dans la Convention (lutte à la pornographie infantile, collaboration avec les fournisseurs, entre les États, etc.)? De plus, il est à noter que la Convention ne permet des réserves limitées que sur quelques-unes de ses dispositions[17].

Si jamais le Canada décidait de ratifier la Convention, celui-ci devrait à tout le moins utiliser son droit de déposer les quelques réserves qui lui serait alors permises :

- Exigence de dommages sérieux dans le cas d'atteintes à l'intégrité des données (art. 4)
- Abus de dispositif (art. 6 : toutefois aucune réserve n'est permise dans les cas de vente ou autre mise à disposition de dispositif)
- Infraction se rapportant à la pornographie infantile (art. 9)
- Certaines réserves limitées relativement à la propriété intellectuelle (art. 10)
- Tentative et complicité (art. 11)
- Limiter la surveillance électronique aux infractions graves (art. 14)
- Réserve permettant la protection des ressortissants canadiens à l'extérieur du pays (art. 22)
- Réserve permettant l'exigence de la double incrimination lors des demandes d'entraide (art. 25)

[14] Robert Ménard, président de *Reporters sans frontière* dans *Dossier, Liberté d'expression sur l'internet*, paru dans le no 112 *Hommes et libertés*, Ligue française des droits de l'Homme, janvier/février 2001.
[15] *R.* c *Zundel*, [1992] 2 R.C.S. 731.
[16] *R.* c *Keegstra*, [1990] 3 R.C.S. 697.
[17] *Convention sur la cybercriminalité*, article 42.

- Réserve relative aux États fédéraux (art. 41). Bien que les télécommunications soient de compétence fédérale, la Convention risque d'avoir un impact sur la santé, l'éducation, etc., ce qui soulèverait éventuellement la question du respect des compétences provinciales.

Quelques interrogations

Le document de consultation et la démarche gouvernementale soulèvent plusieurs interrogations significatives qui sont toujours sans réponse.

- Que signifie « infraction grave » pour le ministère de la Justice? Pourquoi ne pas limiter l'interception aux véritables infractions graves? Pourquoi la torture ne fait-elle pas partie des infractions graves et dans ce cas, pourquoi les agents de l'État ne sont-ils pas soumis à la surveillance?

- Les informations recueillies, y compris les informations sur le trafic, feront-elles partie d'un mégafichier ?

- Qui aura la charge de surveiller l'application des mesures ?

- Qu'y a-t-il de prévu, autre qu'une référence générale à la *Charte canadienne des droits et libertés,* pour la protection à la vie privée, du droit d'expression et du droit d'association ?

- Pourquoi seulement les représentants d'entreprises seraient consultés sur l'élaboration de règlements d'application qui auront un impact direct sur l'exercice des droits et libertés ainsi que sur les échanges quotidiens dans la société civile en général ?

- Lorsque des policiers, ou des personnes désignées par ceux-ci, effectueront des saisies ou interceptions illégales, seront-ils encore protégés par l'immunité prévue à l'article 25.1 et al du Code criminel ? Pourquoi ne pas inclure la **surveillance électronique illégale** parmi les crimes que les agents de l'État et les personnes désignées ne pourront en aucun cas commettre pour fin d'enquête (comme le sont le meurtre, les crimes à caractères sexuels, etc.) ? La mise de côté de l'immunité dans les situations de surveillance électronique serait conforme à la Convention qui, d'une part prohibe l'interception illégale (art. 3), et d'autre part, exige que les pouvoirs et procédures soient soumis à une ***supervision judiciaire ou d'autres formes de supervision indépendante*** (art 15 (2)).

- Comment la personne qui fait l'objet de surveillance pourra-t-elle être informée d'une telle opération et **comment pourra-t-elle rectifier efficacement les données comprenant des informations fausses** ?

- Pourquoi n'y aurait-il pas la formation d'un Comité de surveillance chargé d'examiner les impacts de ces mesures, formé, comme au SCRS, non seulement de représentants de l'entreprise privée mais aussi de la société civile en général ? La Convention prévoit que chacun des États désignera une autorité centrale chargée de saisir rapidement les données informatiques pour le compte d'un État requérant : cet organisme, qui risque d'être dépendant

du ministère de la Défense, devrait être imputable devant le Parlement et la société canadienne.

En conclusion

Depuis les événements du 11 septembre 2001, l'adoption en vrac de toute une série de mesures et de dispositions législatives relatives au terrorisme apporte des modifications qui auront à plus ou moins long terme des répercussions sur l'économie générale de notre système juridique et judiciaire.

Le projet de législation « Accès légal » s'inscrit dans cette perspective et nécessite la tenue d'un débat public éclairé sur l'ensemble des enjeux de société et de droits fondamentaux qu'il soulève.

Et finalement, considérant l'absence de démonstration de la nécessité de ce type de législation, dans une société libre et démocratique, la *Ligue des droits et libertés* demande au gouvernement fédéral de surseoir à son projet « Accès légal ».

Ligue des droits et libertés
Décembre 2002