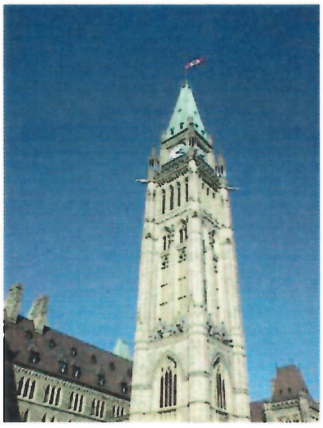
Department of Justice Canada
Ministère de la Justice Canada

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



Nevis Consulting Group Inc.
Directeur de la rédaction

Le 28 avril 2003

Canada

# TABLE DES MATIERES

# CHAPITRE 1: INTRODUCTION

## A. CONTEXTE

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

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

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

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

---

[1] Service canadien du renseignement de sécurité

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

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

[4] Voice over Internet Protocol.

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

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

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

## 2.2 INDUSTRIE

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

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

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

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

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

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

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

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

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

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

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