Ministère de la Justice Canada
Department of Justice Canada

RÉPONSE DU GOUVERNEMENT DU CANADA AU RAPPORT DU SOUS-COMITÉ DE LA CHAMBRE DES COMMUNES SUR LES INFRACTIONS RELATIVES AUX ORDINATEURS

Canada

OCTOBRE 1983

Réponse du gouvernement du Canada
à
la demande du Comité permanent
de la justice et des questions juridiques
portant sur
le dépôt par le gouvernement
d'une réponse globale au
neuvième rapport du Comité
en vertu du paragraphe (13) de l'article 69 du
Règlement de la Chambre des communes

Comme le reconnaît le rapport du sous-comité, la société canadienne évolue vers une économie fondée sur l'information. Une partie importante du produit national brut du Canada et de l'emploi des Canadiens dépend de la production, du traitement, du stockage et de l'utilisation de l'information. Par conséquent, les Canadiens doivent conclure les nouveaux arrangements juridiques, économiques et sociaux qui leur permettront de créer et d'utiliser efficacement la nouvelle information et les nouvelles techniques, qui tiendront compte des valeurs politiques et humaines fondamentales, et ce, en vue d'assurer une protection contre les applications ou les restrictions inconsidérées de cette nouvelle information et de ces techniques.

Le gouvernement félicite le Sous-comité sur les infractions relatives aux ordinateurs pour son étude sur l'informatique et la criminalité informatique et les questions connexes en matière d'information, étude qui aide les Canadiens à comprendre la complexité des questions. Le gouvernement veut répondre aux recommandations dans l'ordre dans lequel elles ont été formulées.

1. **Le Sous-comité recommande de modifier le Code criminel afin de créer deux nouvelles infractions: l'utilisation non autorisée d'un système informatique (sans apparence de droit) et la modification ou la destruction non autorisée (sans apparence de droit) de données informatisées. Le Sous-comité recommande en outre que les avocats de la Couronne aient le choix entre la déclaration sommaire de culpabilité et l'inculpation (par. 37) .**

Le 25 juillet 1983, le ministre de la Justice a rendu public un ensemble de propositions visant à modifier le droit pénal intitulé: " **Avant-Projet de loi modifiant le Code criminel, la Loi modifiant le Code criminel, la Loi relative aux enquêtes sur les coalitions, la Loi de 1977 modifiant le droit pénal, le Tarif des douanes, la Loi sur les aliments et drogues, la Loi sur les stupéfiants, la Loi sur les poids et mesures, abrogeant certaines autres lois et apportant des modifications connexes** ". Ces propositions comprennent deux modifications au **Code criminel** , qui constituent la pièce jointe "A", et qui visent à mettre le droit pénal à jour en ce qui a trait à la protection des systèmes informatiques.

En particulier, il est proposé à l'article 54 de **l'Avant-projet de loi modifiant le Code criminel** et autres, d'ajouter un nouvel article prévoyant comme infraction le fait de, frauduleusement et sans apparence de droit a) obtenir des services d'ordinateur, b) intercepter une fonction d'un ordinateur et c) utiliser un ordinateur dans l'intention de commettre l'une ou l'autre des infractions susmentionnées ou l'infraction de méfait concernant des données ou un ordinateur. Il est proposé à l'article 67 d'ajouter un nouvel article afin d'inclure dans l'infraction de méfait le fait de volontairement a) détruire ou modifier des données, b) dépouiller les données de leur sens, de les rendre inutiles ou inopérantes, c) empêcher, interrompre ou gêner l'emploi légitime des données et d) empêcher, interrompre ou gêner une personne dans l'emploi légitime des données ou refuser l'accès aux données à une personne qui y a droit. Les articles 54 et 67 prévoient que quiconque commet l'une de ces infractions est coupable d'un acte criminel et passible d'un emprisonnement de dix ans ou est coupable d'une infraction punissable sur déclaration sommaire de culpabilité.

Ces propositions sont conformes avec les recommandations du Sous-comité et à plusieurs égards, accordent une plus grande protection des systèmes informatiques. Le ministre de la Justice a l'intention de présenter ces propositions ou des propositions semblables sous la forme d'un projet de loi devant le Parlement au cours de la présente législature.

2. **Le Sous-comité recommande que les définitions nécessaires à la description des infractions portent le plus possible sur les fonctions exécutées et non sur les techniques en cause (par. 38) .**

Le gouvernement convient que toute définition utilisée pour aider à décrire les infractions qui sont proposées doit porter le plus possible, de manière concrète sur les fonctions exécutées et non se fonder sur les techniques actuelles. Par ailleurs, le gouvernement reconnaît le principe fondamental du droit pénal selon lequel la définition des infractions doit être précise et juste de manière à permettre une interprétation convenable des dispositions législatives et à indiquer convenablement au public les activités qui sont précisément interdites. Les définitions et les descriptions des infractions contenues dans le **Projet de loi modifiant le Code criminel** et autres susmentionné, réalisent ces deux objectifs.

3. **Le Sous-comité recommande d'étudier à fond toutes les questions liées à la détection des délits informatiques et aux poursuites contre leurs auteurs, particulièrement en ce qui concerne l'étendue des pouvoirs de perquisitions et de saisies, ainsi que les lois fédérales et les traités portant sur les enquêtes internationales et l'extradition; il y aurait lieu également d'étudier l'application, aux communications entre ordinateurs, les dispositions du Code criminel en matière d'écoute électronique (par. 47) .**

Le ministère de la Justice, le ministère du Solliciteur général, la Commission de réforme du droit du Canada et les ministères du Procureur général des provinces sont actuellement engagés dans une révision en profondeur du droit pénal, révision amorcée par notre gouvernement en 1980. Au cours de cette révision, les pouvoirs de perquisitions et de saisies et les dispositions du **Code criminel** en matière d'écoute électronique seront étudiés et on accordera une attention particulière aux problèmes que pose les techniques informatiques dans ces domaines.

Le ministère de la Justice entend examiner la **Loi sur l'extradition** et la **Loi sur les criminels fugitifs** et se pencher plus particulièrement sur la possibilité de demander l'extradition ou d'extrader quelqu'un relativement à des délits informatiques.

Sur le plan international, le Canada est membre du Comité des politiques d'information, d'informatique et de communications de l'Organisation de coopération et de développement économique (O.C.D.E.) et préside le groupe d'experts sur les flux transnationaux des données. Le Canada a récemment participé à une révision de l'O.C.D.E. des attitudes, des approches et des politiques des pays membres à l'égard de l'informatique et des délits informatiques.

Le 18 novembre 1982, le gouvernement a présenté au Sénat, le projet de loi S-33, un projet de nouvelle **Loi sur la preuve au Canada** . Le projet de loi contient des dispositions portant sur l'admissibilité dans les procédures judiciaires des imprimés d'ordinateur et d'autres éléments de preuves d'origine informatique. Le projet de loi a été présenté en deuxième lecture le 7 décembre 1982 et le 28 juin 1983, le Comité permanent des affaires juridiques et constitutionnelles a publié un rapport provisoire. Conformément au rapport, le ministère de la Justice tient des consultations avec les procureurs généraux des provinces, l'Association du barreau canadien et d'autres groupes et particuliers intéressés en vue de présenter une version modifiée du projet de loi.

4. Le Sous-comité recommande de faire tous les efforts possibles pour veiller à ce que les policiers et les avocats de la Couronne qui pourraient être amenés à s'occuper de criminalité informatique reçoivent une formation leur permettant de s'acquitter efficacement de leurs fonctions (par. 48) .

Depuis juin 1980, le Collège canadien de police à Ottawa a donné neuf cours de techniques d'enquête sur les infractions informatiques qui sont conçus et coordonnés par la Gendarmerie royale du Canada. En tout 180 personnes ont suivi le cours: 109 agents de la Gendarmerie royale du Canada et 71 des autres services de police. Ce cours s'adresse particulièrement aux enquêteurs qui ont de l'expérience

en matière de criminalité des affaires mais qui n'ont pas d'expérience antérieure en informatique. Le cours prépare les candidats à mener des enquêtes sur les actes criminels commis au moyen de l'informatique et leur donne suffisamment de notion sur le milieu informatique pour leur permettre de reconnaître les façons possibles de mener leurs enquêtes.

Le cours est divisé en cinq sujets principaux: les notions portant sur l'informatique et sur les services informatiques, l'introduction à la programmation, la sécurité en matière d'informatique, le droit et la preuve et la criminalité informatique. Le premier sujet permet au personnel du traitement des données de démystifier l'ordinateur. La deuxième partie porte sur les langages informatiques et la programmation. La partie qui porte sur la sécurité des installations informatiques traite du concept de la sécurité des ordinateurs, des systèmes de sécurité et de leurs faiblesses. Les deux dernières parties, le droit et la preuve et la criminalité informatique sont étroitement liées. Les candidats doivent au moyen d'études de cas qui portent sur des problèmes d'affaires fictifs, mener des enquêtes sur des infractions de vol et de fraude, tout en faisant particulièrement attention aux suspects possibles, aux points faibles des systèmes et aux éléments de preuves en vue de les présenter devant les tribunaux. Dans ces cours, on analysera également les affaires nationales et internationales importantes. Le cours est constamment surveillé et modifié pour tenir compte des changements qui se produisent dans le monde de l'informatique.

Les procureurs généraux des provinces sont principalement responsables de l'application du droit pénal et des poursuites relatives à celui-ci. Par conséquent, le gouvernement ne possède pas de données sur l'existence ou l'importance des cours de formation destinés aux services de polices provinciaux et municipaux, et aux procureurs de la Couronne provinciaux. Toutefois, il peut indiquer que le Collège canadien de police offre une certaine formation aux policiers provinciaux et municipaux.

5. **Le Sous-comité recommande que l'industrie de l'informatique et les organismes usagers évaluent les faiblesses de leur système et adoptent les mesures de sécurité nécessaires (par. 51) .**

L'équipe d'inspection et d'évaluation de la sécurité des services informatiques (E.I.E.S.), organisée et administrée par la Gendarmerie royale du Canada est chargée de l'inspection et de l'évaluation des services informatiques du gouvernement aussi que des installations du secteur privé s'occupant, en vertu d'un marché, du traitement de l'information gouvernementale.

La documentation suivante se trouve à la pièce jointe "B": les extraits du Manuel de la politique administrative du Conseil du Trésor sur la sécurité en informatique et les annexes A, B et C de la **Loi sur l'administration financière** . Ces documents décrivent en détail l'engagement du gouvernement dans ce domaine important.

6. **Le Sous-comité recommande de modifier la** Loi sur le droit d'auteur **pour y inclure les logiciels informatiques (par. 55) .**

Les ministres de la Consommation et des Corporations et des Communications étudient actuellement des modifications possibles la **Loi sur le droit d'auteur** dont en autre, des mesures portants sur les logiciels informatiques.

7. **Le Sous-comité recommande que le gouvernement fédéral effectue une étude en profondeur sur la possibilité d'étendre aux programmes informatiques la protection visant les brevets et les dessins industriels (par. 56) .**

La question de la propriété intellectuelle des logiciels informatiques fait actuellement l'objet d'une étude au ministère de la Consommation et des Corporations.

8. **Le Sous-comité recommande aux gouvernements fédéral et provinciaux d'étudier à fond, conjointement, le droit relatif au secret industriel et d'adopter les mesures correctives qui s'imposent (par 58) .**

Le gouvernement désire souligner que les questions relatives à la protection de l'information ne sont pas seulement reliées à l'utilisation des ordinateurs. En juin 1983, le ministère de la Justice de concert avec l' **Institute of Law Research and Reform** de l'Alberta a terminé une étude préliminaire du besoin d'élaborer au Canada une loi d'uniformisation sur la protection en droit civil des secrets industriels et d'autres genres de renseignements commerciaux de nature confidentielle ainsi que les peines de droit pénal qui sont nécessaires pour assurer une telle protection. Le gouvernement propose donc d'engager des discussions avec les provinces quant à l'institution d'une étude fédérale-provinciale portant sur le genre de protection que la loi devrait assurer dans ce domaine.

Le rapport du Comité (aux paragraphes 59 à 62) ne comprend qu'une référence partielle aux mesures législatives fédérales qui prévoient la protection des renseignements personnels détenus par le secteur public fédéral. Pour clarifier cette question, le gouvernement voudrait indiquer que la **Loi sur la protection des renseignements personnels** S.C. 1980-81-82-83, c. 111, contient un code détaillé réglant l'utilisation et la divulgation des renseignements personnels détenus par les institutions du gouvernement fédéral (articles 7 et 8). Ces dispositions sont très semblables à celles qui sont inscrites dans la nouvelle loi du Québec sur l'accès aux documents publics et la protection des données à caractère personnel que le Comité souligne particulièrement. De plus, il existe certaines dispositions sur la confidentialité des renseignements détenus par le gouvernement fédéral dans plus de 53 lois. Un grand nombre d'entre elles traitent des renseignements à caractère personnel tandis que d'autres traitent des renseignements commerciaux de nature confidentielle.

9. Le Sous-comité recommande que l'industrie de l'informatique adopte ses propres règlements pour veiller à ce que ses membres aient une conduite irréprochable (par. 65) .

Le gouvernement appuie les efforts de l'industrie de l'informatique en vue d'établir des principes d'éthique élevés en ce qui concerne l'utilisation des systèmes informatiques et en vue d'appliquer des mesures de sécurité appropriées. La Gendarmerie royale du Canada fournit de l'aide dans ce domaine par l'entremise de l'équipe d'inspection et d'évaluation de la sécurité. De plus, elle poursuit un programme de sensibilisation aux mesures de sécurité des systèmes informatiques en publiant de la documentation relative à la sécurité en matière d'informatique.

10. Le Sous-comité recommande que les professeurs d'informatique soient tenus d'être qualifiés dans le domaine de l'éthique en informatique et que les responsabilités morales liées à l'utilisation d'ordinateurs figurent dans les cours d'informatique de tous les niveaux (par. 67) .

Les législatures provinciales sont en grande partie responsables de l'éducation. Toutefois, le gouvernement est actif dans ce domaine, par l'entremise de la Gendarmerie royale du Canada en donnant des cours sur la sécurité des systèmes informatiques au Collège canadien de police à Ottawa. L'éthique en informatique fait partie intégrante de cette formation. Le gouvernement envisage également que les cours de formation professionnelle sur le fonctionnement des ordinateurs, qui sont parrainés par la Commission de la fonction publique, comprennent une partie sur l'éthique en informatique.

Avant-projet de Loi modifiant le Code criminel, la Loi modifiant le Code criminel, la Loi relative aux enquêtes sur les coalitions, la Loi de 1977 modifiant le droit pénal, le Tarif des douanes, la Loi sur les aliments et drogues, la Loi sur les stupéfiants, la Loi sur les poids et mesures, abrogeant certaines autres lois et apportant des modifications connexes

Canada

54. (1) La même loi est en outre modifiée par insertion, après l'article 301.1, de ce qui suit :

Utilisation non autorisé d'ordinateur

«**301.2** (1) Quiconque, frauduleusement et sans apparence de droit,

a) directement ou indirectement, obtient des services d'ordinateur,

b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur,

c) directement ou indirectement, utilise ou fait utiliser un ordinateur dans l'intention de commettre une infraction prévue à l'alinéa *a*) ou *b*) ou une infraction prévue à l'article 387 concernant des données ou un ordinateur,

est coupable d'un acte criminel et passible d'un emprisonnement de dix ans ou est coupable d'une infraction punissable sur déclaration sommaire de culpabilité.

Définitions

(2) Aux fins du présent article,

«dispositif électromagnétique, acoustique, mécanique ou autre» désigne tout dispositif ou appareil utilisé ou pouvant être utilisé pour intercepter une fonction d'un ordinateur, mais ne comprend pas un appareil de correction auditive utilisé pour améliorer, sans dépasser la normale, l'audition de l'utilisateur lorsqu'elle est inférieure à la normale; «dispositif électromagnétique» "*electromagnetic*"

«donnée» désigne la représentation d'informations ou de concepts qui sont préparés ou l'ont été de façon à pouvoir être utilisés dans un ordinateur; «donnée» "*data*"

«fonction» comprend des fonctions logiques, arithmétiques, des fonctions de commande, de communication de même que des fonctions de mémorisation et de recouvrement ou de relevé des données. «fonction» "*function*"

«intercepter» s'entend au sens de l'article 178.1; «intercepter» "*intercept*"

«ordinateur» signifie un dispositif ou un ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs d'entre eux, «ordinateur» "*computer system*"

a) contiennent des programmes d'ordinateur ou d'autres données, et

b) conformément à des programmes d'ordinateur,

(i) exécutent des fonctions logiques et de commande,

(ii) peuvent exécuter toute autre fonction.

«programme d'ordinateur» signifie un ensemble de données qui représentent des instructions ou des relevés et qui, lorsque traités par l'ordinateur, lui font remplir une fonction; «programme d'ordinateur» "*computer program*"

67. (1) L'article 387 de la même loi est modifié par insertion, après le paragraphe (1) de ce qui suit :

«(1.1) Commet un méfait, quiconque, volontairement,

a) détruit ou modifie des données;

b) dépouille les données de leur sens, les rend inutiles ou inopérantes;

c) empêche, interrompt ou gêne l'emploi légitime des données;

d) empêche, interrompt ou gêne une personne dans l'emploi légitime des données ou refuse accès aux données à une personne qui y a droit.»

(2) Les paragraphes 387(3) à (5) de la même loi sont abrogés et remplacés par ce qui suit :

1972, c. 13, art. 30

«(3) Quiconque commet un méfait à l'égard d'un bien qui constitue un titre testamentaire ou dont la valeur est supérieure à cinq cents dollars est coupable,

Idem

a) d'un acte criminel et passible d'un emprisonnement de dix ans; ou

b) d'une infraction punissable sur déclaration sommaire de culpabilité.

(4) Quiconque commet un méfait à l'égard d'un bien, autre qu'un bien visé au paragraphe (3) est coupable,

Idem

a) d'un acte criminel et passible d'un emprisonnement de deux ans; ou

b) d'une infraction punissable sur déclaration sommaire de culpabilité.

(5) Quiconque commet un méfait à l'égard de données est coupable,

a) d'un acte criminel et passible d'un emprisonnement de dix ans; ou

b) d'une infraction punissable sur déclaration sommaire de culpabilité.

(5.1) Est coupable

Infraction

a) d'un acte criminel et passible d'un emprisonnement de cinq ans, ou

b) d'une infraction punissable sur déclaration sommaire de culpabilité,

quiconque volontairement accomplit un acte ou volontairement omet d'accomplir un acte qu'il a le devoir d'accomplir, si cet acte ou cette omission est susceptible de constituer un méfait qui cause un danger réel pour la vie des gens ou de constituer un méfait à l'égard de biens ou de données.»

(3) L'article 387 de la même loi est modifié par adjonction de ce qui suit :

«(8) Dans cet article, «données» a la même signification qu'à l'article 301.2.»

Définition de «données»

Conseil du Trésor Canada

Manuel de la politique administrative

Chapitre 440, Section 8

Informatique: sécurité

Décembre 1978

Table des matières

.8.1 Objet et portée *3*
.8.2 Champ d'application *4*
.8.3 Rôle et fonctions *4*
.8.4 Directives *6*
.8.5 Lignes directrices *7*
.8.6 Interprétation et avis *9*
.8.7 Références *9*

Définitions clés

Directives: énoncé précisant les éléments obligatoires d'une politique. Lorsque le Conseil du Trésor se montre disposé à permettre certain écarts, les ministères doivent alors lui soumettre une présentation en vue d'obtenir une autorisation préalable. Les directives se distinguent par l'emploi du verbe ***devoir, ou de tout autre verbe d'obligation, au présent ou au futur*** et sont dactylographiées en caractères ***italiques gras***.

Lignes directrices: énoncé précisant des instructions qui, sans être obligatoires, devraient être suivies, à moins qu'il n'existe de sérieuses raisons d'agir autrement. Bien qu'il soit nécessaire d'étayer les raisons de la dérogation aux lignes directrices, on n'a pas besoin d'une autorisation préalable du Conseil du Trésor. Les lignes directrices se distinguent par l'emploi du verbe ***devoir, ou de tout autre verbe approprié, au conditionnel*** et sont dactylographiées en *italiques*.

.8.1 Objet et portée

Les sous-chefs des ministères et les chefs des organismes sont responsables de l'application de mesures de sécurité adéquates au sein de leur ministère ou organisme respectifs. La présente section a pour objet de fournir une direction dans l'exercice de ces responsabilités dans le milieu informatique. Elle est destinée à aider les responsables de la planification et de l'élaboration des mesures de sécurité dans le milieu informatique.

Il est généralement admis que l'infaillibilité n'existe pas dans ce domaine. Le système de sécurité optimal est celui qui permet d'assurer un équilibre entre le coût des mesures de sécurité prises contre un risque donné au cours d'une période de temps déterminée et la probabilité de réalisation du risque et les conséquences, pécuniaires ou autres, que celle-ci entraîne pour l'État. Cet équilibre devrait être atteint pour chaque type de risque d'atteinte à la sécurité de l'information, du personnel ou de l'équipement.

Dans la plupart des situations, en particulier celles auxquelles doivent faire face les administrations publiques, il est extrêmement difficile de déterminer simultanément la probabilité de réalisation d'un risque et les frais qui découlent de cette réalisation. Néanmoins, on ne saurait exagérer l'importance de l'évaluation des risques et de leurs conséquences avant l'adoption des mesures de sécurité appropriées dans tout milieu informatique. Dans la plupart des cas, il est possible d'évaluer, avec une marge de précision de l'ordre de dix, la fréquence prévisible de l'événement et les frais qui découlent de la réalisation d'un risque donné. Ce calcul peut, tout au moins, faciliter la détermination de l'importance qui doit être accordée au système de sécurité.

Les risques dépendent principalement du type d'information manipulée. L'information susceptible d'intéresser une puissance étrangère nécessite évidemment des mesures de sécurité différentes de celles qu'un particulier peut prendre contre son voisin. La continuité du service informatique est certes plus importante pour certains processus particuliers. Toutefois, il est certain que toutes les ressources affectées au traitement des données justifient des mesures de sécurité minimales. La présente section traite, d'une manière générale, des normes de sécurité minimales, et s'applique donc à toutes les installations de traitement des données au sein de l'administration fédérale. A cet égard, certains ministères doivent prendre des mesures plus strictes que celles qui sont énoncées dans la présente section.

Plusieurs aspects de la sécurité en milieu informatique et de la sécurité dans les autres milieux sont communs. Ceux-ci font généralement l'objet de mesures et de pratiques distinctes, elles seront traitées brièvement car des directives sont déjà disponibles auprès des agents de sécurité des ministères et des organismes gou-

vernementaux qui ont des responsabilités particulières dans le domaine de la sécurité.

.8.2 Champ d'application

La présente section a été établie avec l'aide et le concours du Comité consultatif de la sécurité. Elle s'applique aux organismes qui figurent à l'annexe C de la *Loi sur l'administration financière* de même qu'aux ministères et aux organismes énumérés aux annexes A et B ainsi qu'aux directions désignées comme ministères aux fins de ladite loi. Les dispositions de la présente section ne s'appliquent pas au ministère de la Défense nationale, dans le cas où elles sont incompatibles avec les besoins organisationnels et opérationnels de ce ministère, comme il est prévu dans la *Loi sur la Défense nationale*.

.8.3 Rôle et fonctions

Un certain nombre d'organismes et de services sont responsables des divers aspects de la sécurité au sein de l'administration fédérale. Plusieurs responsabilités en matière de sécurité indiquées ci-dessous ne sont pas particulières à l'informatique. Elles sont cependant présentées dans l'intérêt du lecteur. Le résumé qui suit est établi pour la commodité de ce dernier et il ne fait pas autorité.

.8.3.1 *Les sous-ministres et les chefs d'organismes* sont les seuls responsables de la mise en oeuvre et de l'application, au sein de leur ministère ou organisme respectif, des politiques et procédures de sécurité du gouvernement énoncées aux références (a) et (b) de l'article .8.7. Celles-ci comprennent la responsabilité de déterminer le niveau de sécurité nécessaire dans les services informatiques utilisés pour le traitement de l'information de leur ministère ou organisme.

.8.3.2 *L'agent de sécurité du ministère (ASM)* est chargé de veiller, sous l'autorité du sous-ministre ou du chef d'organisme, à la mise en oeuvre, la coordination, la surveillance et la vérification de toutes les politiques, normes et procédures de sécurité, y compris celles qui ont trait à l'informatique au sein de son ministère.

.8.3.3 *Le Comité consultatif de la sécurité (CCS)* est un organisme interministériel qui donne des avis sur des questions de sécurité et qui agit en qualité de conseiller et de guide en cas de conflit au sein de l'administration fédérale.

.8.3.4 *Le Comité interministériel de la sécurité en informatique (CISI)* est un organisme consultatif qui rend compte au CCS et qui se compose des représentants de certains centres d'informatique de l'État. Il est chargé de faire des recommandations et de donner des

avis sur des questions de sécurité relatives aux pratiques en matière d'informatique, d'examiner les activités de l'Équipe d'inspection et d'évaluation de la sécurité en informatique.

.8.3.5 *Le Comité de la sécurité des communications électroniques (CSCE)* est un organisme consultatif interministériel qui rend compte au CCS sur la sécurité des communications de l'État.

.8.3.6 *Le Comité consultatif du matériel de sécurité (CCMS)* est un organisme interministériel qui rend compte au CCS et qui est chargé de toutes les questions ayant trait à la fourniture de matériel approuvé de sécurité à l'usage de l'État.

.8.3.7 *Le Commissaire de la Gendarmerie royale du Canada (GRC)* a la responsabilité de conseiller les sous-ministres et les chefs d'organismes sur la mise en oeuvre des politiques de sécurité gouvernementales énoncées dans les directives, règlements et instructions, conformément aux responsabilités définies dans les présentes directives et lignes directrices. Pour ce faire, il peut, dans une certaine mesure et après entente, obtenir le concours d'autres ministères ou organismes gouvernementaux.

Le Commissaire de la GRC est responsable de l'organisation et des travaux de l'Équipe d'inspection et d'évaluation de la sécurité en informatique.

.8.3.8 *L'Équipe d'inspection et d'évaluation de la sécurité en informatique (EIES)*, constituée et administrée par la GRC conformément aux dispositions de la présente section, et utilisant, dans la mesure du possible, des ressources interministérielles, est chargée de l'inspection et de l'évaluation des services d'informatique de l'État ainsi que des installations du secteur privé s'occupant, en vertu d'un marché, du traitement de l'information gouvernementale.

.8.3.9 *Le ministère des Approvisionnements et Services (MAS)* est chargé de l'approvisionnement des services et équipements d'informatique destinés aux ministères et organismes gouvernementaux et des marchés qui s'y rapportent. Il doit, dans la mesure du possible, s'assurer que la fabrication et la conception des équipements répondent aux normes de sécurité établies par les règlements et lignes directrices de sécurité de l'État. Le MAS est également chargé d'établir les autorisations sécuritaires des installations et du personnel du secteur privé et de prendre des dispositions pour que l'EIES inspecte les services d'informatique du secteur privé.

.8.3.10 *Le Centre de la sécurité des télécommunications (CST)* du ministère de la Défense nationale a été désigné comme organisme national chargé de la sécurité des communications électroniques (COMSEC) et, à ce

titre, il est chargé de la prestation de conseils et d'avis à tous les ministères et organismes fédéraux sur des questions touchant la sécurité des communications électroniques (COMSEC). Les ministères et organismes dont les noms suivent traitent directement avec le CST pour ce qui est des questions touchant le COMSEC: Affaires extérieures, Défense nationale, Communications, Approvisionnements et Services, Gendarmerie royale du Canada, Transports et Bureau du Conseil privé. Tous les autres ministères et organismes suivent les procédures énoncées à l'article .8.3.11 ci- dessous.

.8.3.11 *Le ministère des Communications (MDC)* est chargé de la prestation de conseils et d'avis, sur des questions touchant le COMSEC, à tous les ministères et organismes qui ne sont pas représentés au sein du CST. Il est de plus chargé de la prestation, à tous les ministères et organismes, de services dans le cadre du chapitre 430 qui traite des télécommunications.

.8.3.12 *Le ministère des Travaux publics (MTP)*, lorsqu'il doit faire construire un édifice ou modifier la structure d'un édifice, est à ce titre responsable de la mise en application des normes de sécurité dans la construction, ce qui comprend l'application des codes gouvernementaux de construction fédéraux, provinciaux ou municipaux et des règles sur la prévention des incendies ainsi que la consultation avec la GRC quant aux répercussions dans le domaine de la sécurité.

.8.4 Directives

.8.4.1 ***Les responsabilités et les méthodes générales de sécurité dans le milieu informatique sont énoncées dans les manuels de sécurité des ministères concernés, à moins d'indication contraire dans les présentes directives et lignes directrices.***

.8.4.2 ***Les ministères et les organismes qui utilisent des services d'informatique doivent:***

a) donner aux renseignements une cote de sécurité conformément aux procédures établies et prévoir les conditions auxquelles celle-ci peut être abaissée; et

b) respecter les normes de sécurité applicables pour tous les services d'informatique notamment les services contractuels qui traitent les données du gouvernement.

.8.4.3 ***Les ministères et organismes qui utilisent des services d'informatique privés ou publics traitant les données du gouvernement doivent s'assurer:***

a) que l'information qui leur est confiée, quelle qu'en soit la forme, est protégée au niveau correspondant à la cote de sécurité et accompagnée des mises en garde appropriées; et

b) qu'une évaluation des risques d'atteinte à la sécurité de l'informatique est faite et qu'un rapport d'évaluation exposant les risques qui ont été relevés est établi et tenu à jour.

.8.4.4 *Tout organisme gouvernemental projetant l'établissement, l'acquisition, la modification ou la réinstallation d'une installation, d'un service ou d'un système général d'informatique doit contacter l'agent de la sécurité du ministère (ASM) pendant la phase de planification afin que toutes les autorités concernées soient consultées.*

.8.4.5 *Les ministères et organismes doivent consulter l'Équipe interministérielle d'inspection et d'évaluation de la sécurité (EIES) pour déterminer le statut de leurs installations d'informatique sur le plan de la sécurité.* Les ministères et organismes qui ont conclu ou projettent de conclure des marchés portant sur le traitement d'informations ayant une cote de sécurité ou de renseignements délicats dans des installations d'informatique privées doivent contacter la Direction des services de sécurité du ministère des Approvisionnements et Services qui prendra les dispositions nécessaires pour que l'EIES inspecte ces installations et présente son rapport d'évaluation de la sécurité.

.8.4.6 *Dans les six mois qui suivent la réception d'un rapport d'évaluation de la sécurité, le ministère ou l'organisme doit communiquer son plan d'action à l'EIES pour résoudre les problèmes particuliers signalés dans le rapport et l'informer des mesures qu'il a prises.* Ces rapports sont présentés à l'EIES chaque année par la suite jusqu'à ce que toutes les mesures nécessaires soient prises ou qu'une nouvelle inspection soit faite.

.8.4.7 *La GRC établira un rapport annuel qu'elle soumettra à la Direction de la politique administrative du Secrétariat du Conseil du Trésor relativement à la situation sécuritaire de toutes les installations d'informatique au service de l'État.* Ce rapport s'appuiera sur les résultats de toutes les activités antérieures de l'EIES et tiendra compte des progrès particuliers signalés par les ministères et les organismes au cours de l'année du rapport.

.8.5 **Lignes directrices**

.8.5.1 *Tous les directeurs d'un service d'informatique devraient nommer un coordonnateur de la sécurité en informatique,* qui reçoit des instructions concernant la politique en matière de sécurité de l'ASM et qui fait rapport au directeur sur des questions touchant la sécurité de l'informatique. Le coordonnateur de la sécurité devrait être un cadre supérieur expérimenté dans le domaine de l'informatique dont les fonctions normales exigent la connaissance des opérations informatiques,

tant du point de vue de la gestion que de celui des systèmes. Cette personne devrait également avoir une connaissance générale des principes, des procédures et des difficultés relatifs au domaine de la sécurité.

.8.5.2 *Le coordonnateur de la sécurité devrait notamment*:

a) évaluer périodiquement les risques d'atteinte à la sécurité et établir des rapports pertinents,

b) élaborer des procédures de sécurité en informatique, proposer des mesures de protection et des mesures d'urgence,

c) vérifier périodiquement les dispositifs de sécurité et les mesures d'urgence,

d) signaler les problèmes possibles en matière de sécurité au directeur de l'informatique,

e) informer et motiver le personnel de l'informatique quant au respect des mesures de sécurité.

.8.5.3 *Le coordonnateur de la sécurité en informatique devrait mettre à jour tous les ans (ou plus fréquemment, au besoin), le rapport d'évaluation de la sécurité en informatique*, et il devrait proposer les modifications ou adjonctions aux mesures de sécurité qui touchent les activités d'informatique.

.8.5.4 *L'interrelation des systèmes d'informatique et des services de télécommunications devrait être planifiée avec soin et coordonnée* de façon que la sécurité de l'information en voie de traitement et de transmission soit protégée. Les intéressés devraient obtenir les renseignements nécessaires des autorités compétentes conformément aux articles .8.3.10 et .8.3.11.

.8.5.5 *Tous les critères de sécurité inhérents à un travail d'informatique qui doit faire l'objet d'un marché devraient être inclus dans les demandes de soumission.* L'aptitude des soumissionnaires à répondre aux exigences indiquées devrait être évaluée.

.8.5.6 *L'auteur des données qui doivent être traitées devrait déterminer et indiquer clairement leur cote de sécurité.* L'identification sécuritaire de l'ordinateur est la responsabilité conjointe de l'auteur et du service d'informatique. L'auteur devrait s'assurer que le gestionnaire du service d'informatique connaît les exigences sécuritaires applicables aux sorties. Le gestionnaire du service d'informatique est responsable de l'identification et de la protection des sorties de l'ordinateur, conformément aux instructions de l'auteur.

.8.5.7 *Des mesures de contrôle sur l'entrée, le traitement, la mise en mémoire et la sortie des données, la génération et la mise à jour des programmes ainsi que sur le fonctionnement et le soutien du matériel, devraient être clairement définies dans les procédures d'opérations normales du service d'informatique.*

.8.6 Interprétation et avis

Il incombe à l'Équipe d'inspection et d'évaluation de la sécurité de la GRC d'évaluer le niveau de sécurité des opérations d'informatique de l'État. A cette fin, elle effectue des inspections périodiques des installations utilisées par les divers ministères et organismes. La fréquence des inspections d'un service donné dépend de l'importance sécuritaire des données et de l'information traitées et du rôle stratégique de ce service par rapport aux objectifs et aux priorités d'ensemble de l'État.

A la suite de l'inspection d'un service, l'EIES prépare, à l'intention du sous-chef responsable du service, un rapport d'évaluation où elle indique le genre d'informations que le service peut, selon elle, manipuler et traiter en toute sécurité. Des copies du rapport d'évaluation sont également envoyées à l'ASM ainsi qu'aux directeurs responsables de l'informatique.

Dans le cas des services contractuels fournis par le secteur privé, un rapport d'évaluation est envoyé au directeur de la Direction des services de sécurité du MAS, qui, par la suite, met les résultats à la disposition de l'administrateur de l'organisme privé. Le MAS peut, sur demande, fournir ces résultats aux ministères et organismes qui passent des marchés pour des services d'informatique.

Des copies de tous les rapports de l'EIES sont fournies, sur demande, à la Direction de la politique administrative du Secrétariat du Conseil du Trésor ainsi qu'au président du Comité consultatif de la sécurité.

Dans les soixante jours de la remise d'un rapport d'évaluation de la sécurité, l'EIES communique avec l'ASM du ministère ou de l'organisme en question afin de lui présenter selon les besoins une interprétation des observations et des recommandations et de lui donner son avis. Cette démarche devrait amener la direction du service et le personnel de la sécurité à formuler un plan d'action visant à résoudre les problèmes de sécurité et à donner suite aux recommandations du rapport.

Ce sont les normes de sécurité en informatique préparées sous la direction du CISI, de concert avec le Comité des normes gouvernementales en informatique, qui servent de critères dans le cadre des évaluations de la sécurité.

.8.7 Références

- *Loi sur les secrets officiels* (S.R.C., 1970, chapitre 0-3).
- Chapitre 430, Télécommunications.

ADMINISTRATION FINANCIÈRE

Annexe A

Ministère de l'Agriculture
Ministère des Communications
Ministère de la Consommation et des Corporations
Ministère de l'Emploi et de l'Immigration
Ministère de l'Énergie, des Mines et des Ressources
Ministère de l'Environnement
Ministère des Affaires extérieures
Ministères des Finances
Ministère des Pêches et Océans Canada
Ministère des Affaires indiennes et du Nord canadien

Ministère de l'Industrie et du Commerce
Département des assurances
Ministère de la Justice
Ministère du Travail
Ministère de la Défense nationale
Ministère de la Santé nationale et du Bien-être social
Ministère du Revenu national
Ministère des Travaux publics
Ministère de l'Expansion économique régionale
Ministère des Approvisionnements et Services
Secrétariat d'État du Canada
Ministère du Solliciteur général
Ministère des Transports
Conseil du Trésor
Ministère des Affaires des anciens combattants
1960, c. 41, art. 16; 1963, c. 3, art. 18; 1966-67, c. 25, art. 33; 1967-68, c. 16, art. 13; 1968-69, c. 27, art. 20.

Annexe B

Office de stabilisation des prix agricoles
Commission de contrôle de l'énergie atomique
Commission canadienne de l'emploi et de l'immigration
Directeur de l'établissement de soldats
Directeur des terres destinée aux anciens combattants
Conseil économique du Canada
Office des prix des produits de la pêche
Conseil des recherches médicales
Office du développement et des prêts aux municipalités
Musées nationaux du Canada
Conseil national de recherches du Canada
Conseil de recherches en sciences naturelle et en génie
Conseil des Sciences du Canada
Conseil de recherches en sciences humaines
S.R., c. 116 annexe B; 1957-58, c. 22, art. 15; DORS/63-430, 431; DORS/68-151; DORS/69-257, 305.

Annexe C

Énergie atomique du Canada, Limitée
Société Place du Havre Canada
Société de construction des musées du Canada, Inc.

11

Annexe C (suite)

Société canadienne des postes
Société immobilière du Canada Limitée
Société immobilière du Canada (Mirabel) Limitée
Société immobilière du Canada (Le Vieux Port de Montréal) Limitée
Société immobilière du Canada (Vieux-Port de Québec) Inc.
Les Arsenaux canadiens Limitée
Corporation commerciale canadienne
Commission canadienne du lait
Société de développement de l'industrie cinématographique canadienne
Office canadien des provendes
Canadian National (West Indies) Steamships, Limited
Société canadienne des brevets et d'exploitation Limitée
Office canadien du poisson salé
Corporation des dispositions des biens de la Couronne
Construction de défense (1951) Limitée
Loto Canada Inc.
Commission des champs de bataille nationaux
Commission de la Capitale nationale
Conseil des ports nationaux
Commission d'énergie des Territoires du Nord Canadien
Société immobilière des Travaux Publics Limitée
Monnaie royale canadienne
Uranium Canada Limitée
S.R., c. 116, annexe C; DORS Codif. 1955 Vol. 2, p. 1527; DORS/55-224; C.P. 1960-1684; DORS/63-72; DORS/66-559; DORS/67-230; DORS/68-68; DORS/69-270.