CHAMBRE DES COMMUNES
CANADA

RAPPORT DU SOUS-COMITÉ

SUR LES INFRACTIONS RELATIVES AUX ORDINATEURS

COMITÉ PERMANENT
DE LA
JUSTICE ET DES QUESTIONS JURIDIQUES

JUIN 1983

SOUS-COMITÉ

SUR LES INFRACTIONS RELATIVES AUX ORDINATEURS

PRÉSIDENTE: Mme Céline Hervieux-Payette, Lib., (Montréal-Mercier), Qué.
M. Ken Robinson, Lib., (Etobicoke-Lakeshore), Ontario
L'hon. Perrin Beatty, P.C., (Wellington-Dufferin-Simcoe) Ontario

PERSONNEL

Mme Monique Hébert, Services des recherches, Bibliothèque du Parlement

Pierre de Champlain

Greffier du Sous-comité

CHAMBRE DES COMMUNES

Fascicule nº 18

Le mardi 14 juin 1983
Le jeudi 16 juin 1983
Le mardi 21 juin 1983

Président: Céline Hervieux-Payette

HOUSE OF COMMONS

Issue No. 18

Tuesday, June 14, 1983
Thursday, June 16, 1983
Tuesday, June 21 1983

Chairman: Céline Hervieux-Payette

Procès-verbaux et témoignages du Sous-comité sur

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

Minutes of Proceedings and Evidence of the Sub-committee on

Computer Crime

of the Standing Committee on Justice and Legal Affairs

CONCERNANT:

Ordre de renvoi

RESPECTING:

Order of Reference

Y COMPRIS:

Rapport final

INCLUDING:

Final Report

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

First Session of the
Thirty-second Parliament, 1980-81-82-83

Publié en conformité de l'autorité du Président de la Chambre des communes par l'Imprimeur de la Reine pour le Canada

En vente: Centre d'édition du gouvernement du Canada, Approvisionnements et Services Canada, Ottawa, Canada K1A 0S9

Published under authority of the Speaker of the House of Commons by the Queen's Printer for Canada

Available from the Canadian Government Publishing Center, Supply and Services Canada, Ottawa, Canada K1A 0S9

Le Comité permanent de la justice et des questions juridiques a l'honneur de présenter son

NEUVIÈME RAPPORT

Conformément à son Ordre de renvoi du mercredi 9 février 1983, votre Comité a confié à un Sous-comité l'étude de l'objet du projet de loi C-667, Loi modifiant le Code criminel et la Loi sur la preuve au Canada en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs.

Le Sous-comité a présenté son rapport final au Comité. Votre Comité a adopté ce rapport avec modifications et demande que le gouvernement étudie l'opportunité d'appliquer les recommandations contenues dans le rapport.

Le rapport du Sous-comité, tel que modifié, se lit comme suit:

TABLE DES MATIÈRES

Page

RECOMMANDATIONS 7

INTRODUCTION 9

A. Le phénomène informatique 11

B. Fréquence des délits informatiques 13

C. Le droit pénal : situation actuelle 14

D. Le droit pénal : modifications proposées 15

E. La Loi sur la preuve au Canada 17

F. Les problèmes d'application de la Loi 18

G. Mesures supplémentaires 19

1. Normes de sécurité 19

2. Recours au civil 19

3. Code d'éthique 21

CONCLUSION 23

DEMANDE EN VERTU DU PARAGRAPHE (13) DE L'ARTICLE 69 DU RÈGLEMENT DE LA CHAMBRE DES COMMUNES 23

NOTES 25

ANNEXE «A»: LISTE DES TÉMOINS 27

ANNEXE «B»: BIBLIOGRAPHIE SOMMAIRE 29

RECOMMANDATIONS

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 autorisées (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).

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).

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 perquisition et de saisie, 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, des dispositions du *Code criminel* en matière d'écoute électronique (par. 47).

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).

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

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

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).

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).

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).

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).

INTRODUCTION

1. Le Sous-comité a pour mandat d'examiner les questions visées par le projet de loi C-667, Loi modifiant le *Code criminel* et la *Loi sur la preuve au Canada* en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs.

2. Déposé en première lecture par l'honorable Perrin Beatty le 16 décembre 1982, le projet de loi C-667 a été retiré de la deuxième lecture le 9 février 1983 et renvoyé au Comité permanent de la justice et des questions juridiques. Un sous-comité représentant les trois partis a été créé le 10 mars 1983. Le groupe de travail était en fait composé de la présidente, Me Céline Hervieux-Payette, député, de M. Kenneth Robinson, c.r., député, et de l'honorable Perrin Beatty, député.

3. Selon le Sous-comité, cette façon de procéder a donné des résultats très satisfaisants. Les travaux ont été efficaces et productifs grâce au petit nombre de membres du Sous-comité et à l'atmosphère non partisane qui a régné pendant les délibérations. Pour ces raisons, nous pensons que l'on devrait recourir plus souvent à de petits sous-comités pour l'étude des nombreuses questions qui intéressent le Parlement.

4. Pendant les audiences, qui ont commencé le 17 mars 1983, le Sous-comité a entendu un grand nombre de témoins de professions variées.(1) Ont comparu des particuliers et des groupes spécialisés dans des domaines divers comme les techniques informatiques, la sécurité et la gestion, le droit de l'informatique, le droit de la propriété intellectuelle, l'application de la loi, les milieux bancaires, le droit en matière de protection des renseignements personnels et de protection des consommateurs.

5. Le Sous-comité est profondément reconnaissant à ces personnes qui ont généreusement donné de leur temps et accepté de nous faire profiter de leurs connaissances. Les nombreux points de vue différents présentés au Sous-Comité lui ont été extrêmement utiles et lui ont donné un tableau d'ensemble satisfaisant de bon nombre des questions visées. Le Sous-

comité est particulièrement redevable aux représentants du ministère de la Justice de leur collaboration et à Mme Susan Hubbell Nycum, du cabinet juridique californien *Gaston, Snow and Ely Bartlett*, d'avoir eu l'amabilité de nous faire part de ses constatations sur l'expérience américaine. Le Sous-comité tient également à remercier le greffier du Sous-comité, M. Pierre de Champlain, et Mme Monique Hébert, du Service de recherches de la Bibliothèque du Parlement, pour leur aide pendant les travaux et la préparation du rapport.

La présidente,
Céline Hervieux-Payette

A. Le phénomène informatique

6. Depuis son avènement en 1946(2), l'ordinateur a pris une telle importance dans le traitement de toutes sortes d'informations qu'il est difficile d'imaginer une grande entreprise pouvant fonctionner sans lui. D'après l'industrie, près de 40 millions de dollars sont transférés chaque jour par des systèmes informatiques au Canada. Aux États-Unis, le chiffre atteint près de 400 millions de dollars. À l'échelle mondiale, il s'élève à 600 millions de dollars.(3)

7. Outil indispensable à l'entreprise et au secteur public, l'ordinateur s'introduit maintenant dans les foyers au moyen de consoles de la taille d'une machine à écrire pouvant être branchées sur un écran de télévision. Quiconque possède un compte en banque ou effectue des transactions de crédit utilise régulièrement les services d'un ordinateur. Un témoin a fort à propos donné l'exemple suivant:

> «Aujourd'hui, depuis que j'ai quitté ma maison à Toronto, j'ai été au moins trois fois en contact avec un ordinateur. En début de matinée, j'ai pris l'avion pour Montréal et l'ordinateur d'Air Canada m'a émis ma carte d'embarquement. À midi, j'ai pris le train pour Ottawa et VIA Rail m'a émis un billet par ordinateur. Je me suis ensuite rendu à la Banque de Commerce, j'ai sorti ma carte VISA et j'ai fait un retrait de 100 dollars.»(4)

Bref, l'ordinateur est en train de s'intégrer à toutes les facettes de l'activité humaine. Il peut recueillir, stocker, mettre en corrélation, transférer et extraire des volumes de données considérables avec une facilité et une rapidité relatives. Son utilité actuelle est indéniable, mais les progrès technologiques futurs en feront un outil presque indispensable.

8. Il y a cependant un revers à toute médaille. À cause de l'aptitude de l'ordinateur à traiter de vastes quantités d'informations précieuses, certains y ont vite vu la possibilité tentante de l'utiliser de façon abusive. On a déjà entendu parler des «pirates de l'informatique» qui, avec une connaissance élémentaire du fonctionnement des ordinateurs, s'infiltrent dans des terminaux téléphoniques et des micro-ordinateurs personnels. Dans certaines universités, des «concours» sont organisés pour voir quel étudiant réussira le premier à déjouer les systèmes de sécurité d'un ordinateur, parfois même avec les encouragements du professeur. Des filous de haut vol peuvent escroquer des institutions financières de milliers, voire de millions de dollars, en utilisant l'ordinateur pour virer des fractions de cents sur des comptes fictifs. Des employés mécontents peuvent placer une «bombe logique»* dans le système informatique, bombe à retardement qui «explosera» et détruira des programmes importants après que l'employé aura quitté l'entreprise.

9. Au Canada, deux cas de piratage en particulier ont fait la manchette. D'abord, dans l'affaire de l'école Dalton de 1980, un groupe d'élèves de huitième année d'une école privée de New York s'est servi du micro-ordinateur de l'école pour pénétrer dans les bases de données d'un certain nombre d'entreprises canadiennes et du gouvernement fédéral. Leur

* Une «bombe logique» est un programme, secrètement inséré dans le système informatique, qui permet d'endommager le logiciel ou le matériel dans des conditions déterminées à l'avance. Par exemple, un programmeur du service de la paye pourrait placer une «bombe logique» dans le système d'information sur le personnel: si son nom était un jour supprimé du fichier, ce qui signifierait qu'il a cessé de travailler pour l'entreprise en question, le programme secret serait automatiquement activé et toutes les données sur le personnel en mémoire seraient effacées.

méthode était simple. Grâce à un répertoire de numéros de téléphone d'ordinateurs, ces élèves ont réussi à se brancher sur les ordinateurs canadiens et à s'immiscer dans le réseau tout simplement en essayant tour à tour différents mots de passe jusqu'à ce que l'un d'eux fonctionne. Ils ont fait 21 tentatives de pénétration dans des systèmes informatiques canadiens, mais elles n'ont pas toutes réussi. Certains systèmes étaient très bien protégés au moyen de contrôles et de codes perfectionnés. Deux entreprises seulement ont révélé que leurs banques de données avaient été infiltrées et que des informations y avaient été détruites.

10. Le deuxième cas s'est produit à l'Université de l'Alberta. Pendant l'été 1977, l'ordinateur de l'université a été victime de pannes inhabituellement fréquentes. Soupçonnant une irrégularité, le personnel de l'université a exercé une étroite surveillance et a fini par prendre sur le fait un élève d'école secondaire qui utilisait le système informatique à partir de l'un des terminaux situés sur le campus. L'élève en question n'était pas autorisé à utiliser l'ordinateur. Il a été accusé de méfait en vertu de l'alinéa 287(1)c) du Code criminel(5) et d'utilisation illégale d'une installation de télécommunication en vertu de l'alinéa 287(1)b). Deux autres suspects ont également été accusés de complicité, en vertu du paragraphe 21(1) du *Code criminel*.

11. Lors du procès, un des inculpés a été acquitté faute de preuves suffisantes. Le deuxième, l'élève d'école secondaire pris sur le fait, a été reconnu coupable de deux chefs d'accusation. Le troisième, qui s'appellait McLaughlin, a été reconnu coupable du deuxième chef d'accusation, mais il a été acquitté de l'accusation de méfait étant donné que les preuves réunies n'ont pas permis d'établir sa responsabilité dans les pannes de l'ordinateur.(6) McLaughlin a interjeté appel de son unique condamnation. Dans une décision rendue à deux contre un, la Cour d'appel de l'Alberta a accueilli l'appel et a infirmé la déclaration de culpabilité arguant qu'un système informatique ne constitue pas une «installation de télécommunication». Cette décision a été entérinée par la Cour suprême du Canada.(7)

12. L'affaire *McLaughlin* est importante car elle a révélé que certaines activités, qui seraient autrement considérées comme des infractions, ne constituent pas un acte criminel tout simplement parce que les dispositions actuelles du *Code criminel* présentent des lacunes. Étant donné que les dispositions en question du *Code criminel* ont été rédigées à une époque où les ordinateurs n'existaient pas, leur formulation n'est pas adaptée aux nouvelles techniques. Pourtant, vu les progrès rapides de la technologie, l'ordinateur va sans doute jouer un rôle croissant dans nos vies quotidiennes. Il est manifestement nécessaire de prendre des mesures législatives pour tenir compte de cette nouvelle technologie et protéger la société de ses conséquences négatives. Vu l'aptitude de l'ordinateur à traiter des volumes considérables d'informations précieuses à caractère commercial ou personnel, des mesures appropriées doivent être prises dès maintenant avant que quiconque ne subisse des pertes importantes d'argent ou de données à caractère personnel.

13. Les témoins qui ont comparu devant le Sous-comité sont convenus qu'il est nécessaire de prévoir des sanctions pénales pour combler les lacunes qu'a fait apparaître l'affaire *McLaughlin*. Néanmoins, on s'entend fort peu sur la forme de ces sanctions. Certains témoins sont d'avis que les sanctions pénales ne devraient constituer qu'une des solutions possibles et qu'il faudrait également améliorer les recours existants ou en créer de nouveaux. Cette opinion est partagée par les membres du Sous-comité. Selon nous, il est important d'examiner et d'appliquer tous les recours possibles lorsqu'ils sont appropriés, de façon à réserver les sanctions pénales aux cas extrêmes.

14. Il y a lieu de préciser ici que l'expression «criminalité informatique» est impropre. Elle a l'avantage d'être brève, mais il serait plus approprié de parler de délits «liés à l'informatique». De plus, étant donné que tout acte anti-social considéré comme criminel par nature ne constitue pas un «acte criminel» au Canada à moins qu'il ne soit interdit par la loi, il s'ensuit qu'il serait plus approprié d'utiliser des expressions comme «actes répréhensibles associés à l'informatique» ou «actes répréhensibles liés à l'informatique». En fait, le Sous-comité a pour mandat de proposer des modifications au *Code criminel* afin que les «actes répréhensibles liés à l'informatique» qui ne sont pas proscrits actuellement deviennent des actes criminels. Cela dit, nous emploierons dans le reste de ce rapport les expressions «criminalité informatique» et «délit informatique» par souci de simplicité, que l'acte répréhensible en question constitue ou non un acte criminel.

B. Fréquence des délits informatiques

15. La fréquence des délits informatiques est difficile à estimer. Certains chiffres sont quelque peu excessifs parce que n'importe quel acte répréhensible associé de loin avec un ordinateur est souvent qualifié de délit informatique. Par exemple, si un employé de banque malhonnête falsifie manuellement des documents financiers qui sont par la suite stockés dans l'ordinateur de la banque, cette forme de détournement de fonds n'est plus appelée une fraude. Au lieu de cela, on considère qu'il y a délit informatique, quel que soit le rôle de l'ordinateur dans la perpétration de l'infraction. De la même façon, lorsqu'une personne obtient frauduleusement des fonds d'un guichet de banque automatique grâce au vol d'une carte de crédit et à l'obtention frauduleuse du mot de passe correspondant, cette infraction est une fois encore décrite comme un délit informatique, et non comme le simple vol d'une carte de crédit. Autrement dit, on a généralement tendance à conférer un caractère sensationnel à des infractions par ailleurs assez communes.

16. La fréquence des délits informatiques est aussi assez mal connue parce que certains délits passent parfois inaperçus ou, s'ils sont découverts, parce qu'ils ne sont pas signalés étant donné que les victimes, particulièrement dans le monde des affaires, préfèrent parfois éviter toute publicité négative. Il arrive également que les victimes estiment que le problème peut être le mieux réglé au niveau interne ou que les pertes subies sont simplement trop faibles pour justifier la prise de mesures importantes.

17. Il existe très peu de données empiriques prouvant de façon probante que la criminalité informatique constitue un grave problème. La Sûreté provinciale de l'Ontario a effectué une enquête auprès de 648 sociétés entre 1980 et 1981. Sur 321 répondants, seulement 13 ont signalé des pertes par délit informatique. Il s'agissait dans les deux tiers des cas de vols de temps-machine et de dommages volontaires à des fichiers ou à du matériel informatiques. Seulement cinq cas on été signalés à la police à l'époque, et uniquement trois poursuites semblent avoir été intentées.(8)

18. Les représentants de l'Association des banquiers canadiens ont témoigné qu'à leur connaissance, aucun des membres de leur Association n'a jamais été victime d'un délit informatique «pur», c'est-à-dire d'un délit où l'ordinateur a servi de moyen de perpétration de

l'infraction, et non d'accessoire. Selon d'autres sources, 75 cas approximativement sont signalés tous les ans à l'échelle mondiale, représentant des pertes annuelles totales d'environ 40 millions de dollars.(9)

19. Ces témoignages contredisent catégoriquement la théorie de la «pointe de l'iceberg» selon laquelle 85% de tous les délits informatiques ne sont jamais signalés et représentent des pertes annuelles approximatives de milliards de dollars. Les témoignages entendus par le Sous-comité ne permettent pas d'étayer cette estimation. Il est sans doute plus sûr de conclure que la fréquence réelle des délits informatiques est tout simplement inconnue. Aucune étude exhaustive n'a jamais été effectuée au Canada pour l'estimer, et nous ne pensons pas que cela soit nécessaire pour le moment. À notre avis, le manque relatif d'informations sur la fréquence et la gravité des délits informatiques ne justifie pas l'inaction sur le plan législatif. Il faut quand même se préoccuper de leurs conséquences destructrices pour la société et prendre des mesures législatives pour interdire les actes répréhensibles et décourager les fraudeurs.

C. Le droit pénal: situation actuelle

20. Sur le plan théorique, on peut aborder la question de la criminalité informatique en établissant une distinction entre la notion d'ordinateur comme instrument du délit et la notion d'ordinateur comme objet du délit.

21. Dans la première catégorie, l'ordinateur est utilisé pour commettre l'infraction. L'infraction elle-même n'est pas nouvelle; seul le moyen utilisé pour la commettre l'est. Les plus importantes infractions tombant dans cette catégorie sont les fraudes réalisées au moyen d'un ordinateur: il s'agit d'infractions pour lesquelles des poursuites ont été intentées avec succès par l'application des dispositions actuelles du *Code criminel*.

22. La deuxième catégorie, où l'ordinateur est l'objet du délit, n'est pas si précise. Elle englobe les délits «matériels», où des dommages tangibles sont causés à un ordinateur ou à ses éléments, ou bien lorsqu'il y a vol de ceux-ci. Cette catégorie comprend le vol et le méfait classiques. Les contrevenants sont facilement poursuivis en vertu des mesures législatives actuelles.

23. Le vrai problème se pose lorsque l'ordinateur, en tant qu'objet du délit, n'est victime d'aucun dommage tangible, comme ce fut le cas dans l'affaire *McLaughlin*. On se souviendra que McLaughlin a été acquitté de l'inculpation de méfait parce que les preuves étaient insuffisantes pour établir sa responsabilité dans les pannes de l'ordinateur. Si rien ne vient gêner le fonctionnement ou l'exploitation légitimes de l'ordinateur, ou l'utilisation de l'ordinateur par ses usagers autorisés, il y a peu de chances d'obtenir une condamnation en vertu des dispositions du *Code criminel* sur le méfait.

24. On a tenté récemment d'appliquer à ce genre d'activité les dispositions générales du Code criminel sur le vol. Dans l'affaire *R. c. Stewart*(10), la Couronne a soutenu que l'inculpé était coupable d'avoir conseillé le vol de données appartenant à un hôtel, le plaignant, parce que l'inculpé avait tenté d'obtenir d'un employé de l'hôtel une copie de la liste mécanographique des employés contenant leur nom, leur adresse et leur numéro de télé-

phone. Cette liste mécanographique devait apparemment être utilisée pour syndiquer les employés de l'hôtel.

25. En première instance, le juge n'a pas retenu les arguments de la Couronne soutenant que l'expression «quelque chose», qu'il s'agisse de quelque chose de tangible ou d'intangible, utilisée dans l'article 283 du *Code criminel* sur le vol, devait représenter «quelque chose» pouvant être considéré comme un bien. Des renseignements confidentiels comme une liste d'employés ne sont pas considérés comme un bien aux fins de la loi sur le vol. Quiconque se contente de prendre ou de falsifier des données confidentielles ne prend ni ne falsifie «quelque chose» en vertu de l'article 283.

26. Étant donné que la Cour suprême du Canada a éliminé la possibilité d'assimiler les ordinateurs à des installations de télécommunication, toutes sortes d'activités constituant une violation de systèmes informatiques ne sont pas proscrites.

27. Ces actes répréhensibles qui ne sont pas interdits par le *Code criminel* englobent des activités fort diverses. Celles-ci vont des frasques relativement sans conséquences de plaisantins qui s'amusent à s'immiscer dans les banques de données des autres ou à les découvrir sans intention de modifier ou de détruire les données, jusqu'à l'espionnage industriel, plus grave et plus complexe, où un concurrent copie, sans laisser de traces, des renseignements stockés sur ordinateur qui non seulement sont confidentiels, mais ont une grande valeur, par exemple des données sur d'importants projets de mise en valeur de terrains ou sur de nouvelles découvertes de pétrole. Même si l'information en soi n'a aucune valeur monétaire, les risques de dommages peuvent être élevés. Par exemple, un individu sans scrupules pourrait obtenir accès à des fichiers informatiques sur des employés et utiliser ces renseignements à des fins impropres.

28. Quelle que soit la gravité des actes en question, le Sous-comité estime qu'il faut prévoir des sanctions pénales pour les réprimer, opinion généralement partagée par tous les témoins qui ont comparu devant lui. Néanmoins, on ne s'entend pas vraiment sur la nature exacte de la réforme nécessaire.

D. Le droit pénal: modifications proposées

29. Selon certains témoins, la définition du terme «bien» devrait être étendue afin d'englober «l'information» ou «l'information stockée sur ordinateur», de telle sorte que les dispositions actuelles du *Code criminel* puissent s'appliquer. Le Sous-comité conteste cette approche. À son avis, il serait malavisé d'assortir de droits de propriété l'information en tant que telle, car cette notion n'existe même pas dans le droit civil. Pour des raisons de politique publique, la propriété exclusive de l'information qui découlerait nécessairement de l'application, aux données, de la notion de «bien», s'inscrit mal dans notre système socio-juridique. L'information est considérée comme un bien public trop important pour qu'on en fasse la propriété exclusive de quiconque.

30. Même dans la législation relative aux droits d'auteur, aux brevets, aux marques de commerce et aux dessins industriels, l'inventeur, le créateur ou le concepteur de l'oeuvre n'a pas de droits de propriété exclusifs sur sa création, son invention ou son dessin. Les droits

accordés se rapprochent davantage d'un droit d'exploitation valable pendant une période limitée. Par exemple, en vertu de la *Loi sur le droit d'auteur*(11), l'auteur d'un livre a le droit exclusif de «produire ou reproduire» son livre. Par contre, rien n'empêche d'autres personnes de s'en inspirer. Il est simplement interdit d'en faire des copies ou de le plagier, car il s'agit là d'un droit exclusif de l'auteur et de ses cessionnaires, et ce pendant la vie de l'auteur, plus une période de 50 ans après sa mort. Des considérations analogues quoique pas tout à fait identiques entrent en jeu en ce qui concerne les autres monopoles prévus dans la loi. Pour ces raisons, nous pensons que l'extension de la définition de «bien» afin d'englober «l'information» pourrait entraîner davantage de problèmes qu'elle n'en résoudrait.

31. Deuxièmement, cette mesure est à déconseiller parce qu'elle conférerait à l'information stockée sur ordinateur un statut différent de l'information consignée par des méthodes classiques. Nous ne sommes pas convaincus que la nature du stockage doit influer sur la protection juridique accordée. Des renseignements prélevés dans un classeur ou un ordinateur sont des renseignements volés. À notre avis, par souci de logique, toutes les informations doivent être traitées de façon uniforme, quel qu'en soit le support.

32. Il serait également possible d'élaborer une loi entièrement distincte qui porterait sur toutes les questions liées à l'informatique. Cette possibilité, qui n'a été recommandée par aucun des témoins qui ont comparu devant nous, pose des problèmes pour plusieurs raisons. D'abord, l'élaboration d'une loi satisfaisante nécessiterait beaucoup plus de temps et un surcroît de travail pour en arriver à une bonne vue d'ensemble de la situation. À notre avis, il est plus important d'introduire des modifications restreintes que d'attendre l'élaboration d'une loi générale. Deuxièmement, pour les raisons précitées, il serait peu souhaitable de traiter les délits informatiques différemment des autres actes criminels. Si l'acte en question est de nature criminelle, il doit logiquement relever du *Code criminel*. Enfin, le Parlement n'a probablement pas la compétence législative nécessaire pour adopter une telle loi, étant donné les conflits possibles avec les domaines de compétence provinciale en matière législative.

33. L'idée la plus répandue chez les témoins consisterait à ajouter des dispositions distinctes au *Code criminel* pour protéger spécifiquement l'inviolabilité des ordinateurs. Une de ces dispositions définirait comme un acte criminel le fait d'utiliser un système informatique sans autorisation. Dans une proposition soumise au Sous-comité, l'Association du barreau canadien suggère le libellé suivant: «Quiconque, sans apparence de droit, utilise un système informatique ou une partie d'un tel système sans l'autorisation du propriétaire» commet un acte criminel. D'autres variantes ont été proposées, bien qu'elles n'aient pas été rédigées sous la forme d'articles de loi. Il s'agirait de considérer comme une infraction le fait d'entraver le fonctionnement d'un ordinateur sans autorisation légitime, d'utiliser illégalement un ordinateur, de prendre des données sans autorisation ou d'obtenir des services informatiques sans autorisation.

34. Un certain nombre de témoins ont recommandé de créer une deuxième infraction afin d'interdire les actes plus répréhensibles consistant à modifier des données après avoir obtenu accès à l'ordinateur. À cet égard, l'Association du barreau canadien recommande que l'on définisse une autre infraction qui serait le délit commis par «quiconque, sans apparence de droit, modifie ou détruit des programmes ou des logiciels informatiques sans l'autorisation du propriétaire». Cette formulation, qui vise la question de la modification ou de la destruction de données, reflète assez bien les vues de ceux qui sont en faveur de la création d'une infraction additionnelle.

35. Globalement, le Sous-comité est favorable à cette approche. On pourrait néanmoins soutenir qu'il existerait déjà un délit simple «d'utilisation non autorisée» et qu'il serait possible de tenir compte de la gravité de l'infraction en donnant le choix entre l'inculpation et la déclaration sommaire de culpabilité, et en prévoyant une vaste gamme de peines.

36. Le Sous-comité n'est pas en faveur de cette dernière proposition. Selon lui, les questions d'ordre pratique doivent passer après les exigences de précision et d'équité du droit pénal. À notre avis, la différence entre les deux genres d'actes est trop grande pour qu'ils puissent être traités sur la foi d'une même preuve.

37. Le Sous-comité recommande par conséquent 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 autorisées (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.

38. Le Sous-comité ne tient à aucune formulation particulière. Cependant, nous avons été mis en garde à maintes reprises contre le danger qu'il y aurait à établir des définitions à partir des techniques actuelles. En effet, les progrès étant extrêmement rapides dans le domaine de l'informatique, il est essentiel d'éviter les termes techniques susceptibles d'être rapidement dépassés. Nous recommandons donc que les définitions nécessaires à la description des diverses infractions portent le plus possible sur les fonctions exécutées et non sur les techniques en cause.

39. Comme nous l'avons déjà souligné, on connaît très mal l'ampleur du problème de la criminalité informatique. Afin de corriger cet état de choses, certains proposent d'adopter des dispositions législatives obligeant à signaler ces délits. Le Sous-comité n'est pas en faveur de cette approche. Le *Code criminel* ne comprend guère de dispositions de ce genre, même pour les crimes les plus graves comme l'homicide. Il serait donc selon nous injustifiable que la loi oblige à signaler les délits informatiques si elle ne l'exige pas pour la plupart des autres infractions. Par ailleurs, il serait malaisé d'adopter une disposition de ce genre car il serait très difficile de la faire respecter.

E. La Loi sur la preuve au Canada

40. Le Sous-comité avait notamment pour mandat d'étudier la possibilité de modifier la *Loi sur la preuve au Canada*. L'article 6 du projet de loi C-667 propose en effet de modifier cette loi de façon que les états mécanographiés (imprimés d'ordinateur) soient admissibles en preuve au même titre que les documents originaux.

41. Cette modification semble avoir été proposée en réponse à l'affaire *R. c. McMullen*.(12) Dans cette cause, qui date de 1979, la Cour a statué que, pour que des imprimés d'ordinateur soient recevables, l'ensemble de la preuve doit refléter tout le processus de tenue des dossiers (c'est-à-dire, dans le cas des imprimés d'ordinateur, toutes les procédures à suivre pour l'introduction, le stockage, l'extraction et la présentation de l'information), et que si les gestionnaires, les comptables ou le personnel chargés des dossiers en cause étaient incapables de produire cette preuve, les imprimés d'ordinateur n'étaient pas admissibles.

42. Ce jugement n'a pas été très bien reçu, particulièrement au sein des institutions financières. Non seulement permettait-il l'introduction de preuves susceptibles de nuire à la sécurité de leurs installations informatiques, puisqu'il exigeait la description des procédures à suivre, mais il obligeait en outre trop d'employés de banque à s'absenter du travail pour témoigner.

43. L'affaire *McMullen* semble être passée au second plan lorsqu'un jugement a été rendu dans l'affaire *R. c. Bell and Bruce*.(13) Dans cette affaire, le juge a décidé que les imprimés d'ordinateur constituent des «registres», au sens où l'entend le paragraphe 29(2) de la *Loi sur la preuve au Canada*, puisque ce sont les seules sources de référence dont les banques disposent pour connaître l'état de leurs comptes. À titre de «registres», au sens où l'entend le paragraphe 29(2), les imprimés d'ordinateur ont donc été jugés admissibles sur la foi d'une déclaration sous serment.

44. Depuis le jugement *Bell and Bruce*, les difficultés soulevées par l'affaire *McMullen* semblent s'être résolues d'elles-mêmes dans la pratique, bien que les juristes ne s'entendent pas encore sur l'importance à accorder au jugement *Bell and Bruce* par rapport au jugement *McMullen*.

45. Le Sous-comité a entendu très peu de témoignages sur cet aspect de son mandat. Le 18 novembre 1982, le gouvernement a déposé le projet de loi S-33, intitulé «Loi donnant effet pour le Canada à la Loi uniforme sur la preuve adoptée par la Conférence canadienne de l'uniformisation du droit». Ce projet de loi, qui traite notamment de l'admissibilité des imprimés d'ordinateur, est devant le Comité sénatorial permanent des affaires juridiques et constitutionnelles. Nous n'avons donc pas l'intention de faire de recommandations précises: nous sommes en effet convaincus que les problèmes que risque de poser l'admissibilité en preuve des imprimés d'ordinateur sont étudiés avec toute l'attention qu'ils méritent. Nous tenons néanmoins à souligner l'importance des travaux du Comité sénatorial.

F. Les problèmes d'application de la loi

46. Par leur nature même, les délits informatiques sont difficiles à détecter. Selon les témoignages présentés au Sous-comité, il semble que dans bien des cas, leur découverte soit purement et simplement une question de chance. Puisqu'il est à ce point complexe de détecter les délits informatiques, de recueillir des preuves et de poursuivre les auteurs de ces délits, particulièrement dans le cas du transfert transfrontalier de données, il est essentiel de perfectionner les procédures permettant de le faire.

47. Le Sous-comité recommande par conséquent 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 perquisition et de saisie, 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, des dispositions du *Code criminel* en matière d'écoute électronique.

48. Il ne suffit toutefois pas d'améliorer les techniques d'application de la loi et les pouvoirs connexes pour résoudre efficacement le problème de la criminalité informatique. Il faut aussi que le personnel chargé de détecter les délits informatiques et de poursuivre leurs

auteurs ait une connaissance suffisante du domaine. Les systèmes informatiques sont en effet très complexes, et les néophytes sont facilement dépassés. Le Sous-comité recommande par conséquent 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.

G. Mesures supplémentaires

1. Normes de sécurité

49. Comme nous l'avons déjà souligné, le Sous-comité est fermement convaincu que le droit pénal ne doit constituer qu'une des solutions possibles au problème de la criminalité informatique. Parmi toutes les autres options qui nous ont été présentées, nous estimons que les plus importantes sont celles qui touchent les mesures de sécurité.

50. Selon les témoignages entendus au cours des audiences, il semble que bon nombre des délits informatiques auraient pu être évités si des mesures de sécurité efficaces avaient été appliquées. Il est évident que l'industrie doit adopter ses propres règlements. Selon nous, tous les systèmes informatiques dans lesquels sont stockées des données ayant une certaine valeur, du point de vue commercial ou personnel, doivent respecter des normes de sécurité adéquates.

51. Le Sous-comité ne recommande pas, pour le moment, de normes de sécurité obligatoires, bien que certains témoins l'aient proposé. Il se pourrait bien que la nécessité d'adopter des règlements en ce sens s'impose d'elle-même plus tard. En attendant, nous recommandons que l'industrie de l'informatique et les organismes usagers évaluent les faiblesses de leurs systèmes et adoptent les mesures de sécurité nécessaires.

2. Recours au civil

52. Les recours au civil constituent un complément important aux dispositions du droit pénal. Dans de nombreux cas, les victimes de délits informatiques ne tiennent pas particulièrement à ce que les auteurs de ces délits soient poursuivis au criminel, préférant intenter une action civile afin d'être indemnisées de leurs pertes. Par exemple, si quelqu'un vole un programme de jeu vidéo et vend ensuite des jeux pirates, le créateur du programme peut préférer être indemnisé, plutôt que d'envoyer le voleur en prison. Cette dernière solution n'apporterait en effet pas grand-chose à une victime que cet acte de «piraterie» aurait mis au bord de la faillite.

53. Au niveau fédéral, les dispositions relatives aux monopoles légaux visant le droit d'auteur, les brevets, les dessins industriels, et les marques de commerce sont les seuls recours au civil. Les lois sur le droit d'auteur et sur les brevets semblent les plus susceptibles d'être utiles aux victimes de délits relatifs à des logiciels informatiques. L'opinion semble cependant favoriser la protection par le droit d'auteur.

54. Les logiciels informatiques ne figurent pas expressément au nombre des oeuvres protégées par l'actuelle *Loi sur le droit d'auteur*. Dans la pratique, bon nombre de créateurs demandent cette protection pour leurs programmes mais la loi n'est pas claire à ce sujet. Un certain nombre de spécialistes de la question nous ont affirmé que, selon eux, le droit d'auteur est le meilleur moyen de protection. En 1978, les États-Unis ont modifié leurs lois

sur le sujet afin d'y inclure les logiciels informatiques après qu'un comité présidentiel eut longuement étudié l'application du droit d'auteur aux techniques de pointe.

55. Le Sous-comité tient à souligner qu'au Canada, la révision de la *Loi sur le droit d'auteur* en est actuellement à sa dernière étape. Convaincus que les victimes des délits informatiques devraient avoir autant de possibilités de recours que possible, nous estimons que la protection par le droit d'auteur devrait être étendue aux logiciels informatiques. Nous recommandons par conséquent de modifier la Loi sur le droit d'auteur pour y inclure les logiciels informatiques.

56. Les dispositions sur les brevets et les dessins industriels peuvent elles aussi offrir des possibilités pour la protection des programmes informatiques. En raison du petit nombre de témoignages entendus à ce sujet, le Sous-comité a décidé de ne pas se prononcer sur la question pour le moment. Nous recommandons cependant 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.

57. Le droit relatif au secret industriel est aussi peu précis que celui qui se rapporte aux monopoles légaux du gouvernement fédéral. À l'heure actuelle, la protection du secret industriel, qui n'est prévue qu'en *common law*, est assez efficace lorsqu'il existe clairement un lien *confidentiel* entre deux parties, par exemple dans le cas d'un employé tenu de garder secrète une information reçue dans l'exercice de ses fonctions. Cette protection est cependant moins bien définie lorsque des secrets industriels sont communiqués à une tierce partie qui ne s'était pas engagée à l'origine à garder le secret.

58. Le Sous-comité considère que le droit relatif au secret industriel pourrait être considérablement amélioré pour offrir une meilleure protection à toutes les personnes dont les secrets ont été violés, que ce soit par des moyens informatiques ou autrement; les pertes dues aux vols de secrets industriels peuvent en effet être considérables. À l'heure actuelle, cette question relève des provinces, et aucune d'entre elles n'a encore adopté de loi sur le sujet. Il se pourrait qu'il soit nécessaire plus tard de faire du vol de secrets industriels un acte criminel. Le Sous-comité recommande néanmoins 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.

59. Étant donné les extraordinaires possibilités de l'ordinateur dans les domaines de la collecte et du traitement de données, bien des gens s'inquiètent de la menace que l'ordinateur pourrait constituer pour les données confidentielles à caractère personnel. Les défenseurs de la vie privée ont même recommandé de tenir criminellement responsables les personnes préposées à la garde de données à caractère personnel dans le cas où quelqu'un obtiendrait illégalement accès à ces données en raison de l'insuffisance des mesures de sécurité. Le Sous-comité comprend leur inquiétude, mais il ne peut pour le moment appuyer des mesures aussi draconiennes. Cependant, il faudrait prendre des dispositions pour que les données à caractère personnel, qu'elles soient stockées ou non dans un ordinateur, soient suffisamment protégées de tous ceux qui n'ont pas le droit d'y avoir accès.

60. La protection de la vie privée relève dans une large mesure des autorités provinciales, mais aucune province n'a encore pris l'initiative d'adopter des mesures législatives générales pour protéger toutes les données à caractère personnel, sauf le Québec, qui s'est doté

d'une loi innovatrice sur l'accès aux documents publics et la protection des données à caractère personnel.(14)

61. La loi québécoise est fondée sur le principe que toute information détenue par le secteur public doit être considérée comme confidentielle à moins que la personne concernée n'autorise sa divulgation. Le gouvernement peut adopter des règlements fixant des normes de sécurité destinées à veiller à ce que cette information demeure confidentielle. Par ailleurs, des peines sont prévues pour toute divulgation illégale de données à caractère personnel détenues par le secteur public.

62. Il existe dans d'autres lois fédérales et provinciales certaines dispositions sur la confidentialité des renseignements à caractère personnel, par exemple, au niveau fédéral, les articles 62 et 63 de la *Loi sur la protection des renseignements personnels* et l'article 241 de la *Loi de l'impôt sur le revenu*(15), mais aucune loi globale sur le sujet n'a jamais été adoptée. À notre avis, il y aurait lieu d'étudier plus en profondeur cet aspect peu développé de la législation.

3. Code d'éthique

63. L'industrie de l'informatique étant relativement nouvelle, il y existe très peu de mesures destinées à régir les activités des personnes qui travaillent avec des ordinateurs. Bien que l'information contenue dans ces ordinateurs ait souvent une valeur inestimable ou un contenu confidentiel, il n'y a dans ce domaine aucun code de déontologie obligatoire comme c'est le cas dans d'autres disciplines, par exemple le droit et la médecine. L'Association canadienne des entreprises de services en informatique (CADAPSO) a établi un code d'éthique exposant des normes de comportement dans l'intérêt public et des dispositions sur les relations avec les non-membres assurant des services de traitement des données(16). Il n'est cependant pas nécessaire d'être membre de la CADAPSO pour assurer des services en informatique.

64. L'Association canadienne de l'informatique (ACI) est en train d'établir un processus d'accréditation des programmeurs de systèmes afin que l'industrie puisse réglementer ses propres membres. Ce processus est encore loin d'être terminé.(17)

65. Le Sous-comité appuie ces efforts qui dissuaderont peut-être les auteurs de délits en puissance et inculqueront des principes d'éthique aux usagers des ordinateurs. Si l'industrie ne se réglemente pas elle-même, il se pourrait bien que des mécanismes d'accréditation obligatoire ou d'octroi de permis doivent être envisagés plus tard, mais la situation actuelle ne justifie cependant pas de mesures de ce genre. Le Sous-comité recommande par conséquent que l'industrie de l'informatique adopte ses propres règlements pour veiller à ce que ses membres aient une conduite irréprochable.

66. On se rend de plus en plus compte que les usagers des systèmes informatiques ne sont pas toujours conscients de leurs responsabilités sur le plan de l'éthique. Le problème est particulièrement notable chez les adolescents et les jeunes étudiants dont la maturité d'esprit est parfois beaucoup moins développée que leurs connaissances en informatique.

67. Le Sous-comité considère donc qu'il serait très utile d'inclure des notions d'éthique dans tout programme de formation en informatique. L'enseignement de valeurs morales aux usagers, dès le début, est peut-être un autre moyen de combattre la criminalité informatique. Le Sous-comité recommande par conséquent 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.

CONCLUSION

68. Dès le début de ses travaux, le Sous-comité s'est rendu compte qu'il était impossible de séparer la criminalité informatique de l'«information» en général. Pour cette raison, nous avons fait des recommandations qui pourraient facilement dépasser notre mandat, limité à la criminalité informatique et au droit pénal. Nous estimons cependant qu'il est souhaitable de prévoir tous les recours possibles, la modification du *Code criminel* n'étant qu'une solution parmi tant d'autres. Quant à l'effet de dissuasion, la possibilité de poursuivre en dommages et intérêts les auteurs de délits informatiques peut être aussi efficace que l'imposition d'une amende ou d'une peine de prison.

69. Il est par conséquent nécessaire d'améliorer les recours afin d'offrir aux victimes des délits informatiques la forme de réparation la plus appropriée. Cependant, ces mesures n'entrent en jeu qu'une fois le délit commis. À notre avis, il est plus important de veiller à ce que toutes les mesures préventives possibles soient soigneusement appliquées. Si les systèmes informatiques sont bien protégés et si leurs usagers sont convenablement formés, on pourra prévenir un bon nombre d'actes répréhensibles qui seraient autrement commis.

DEMANDE CONFORMÉMENT AU PARAGRAPHE (13) DE L'ARTICLE 69 DU RÈGLEMENT DE LA CHAMBRE DES COMMUNES

70. Conformément au paragraphe (13) de l'article 69 du *Règlement de la Chambre des communes, articles permanents et provisoires*, le Comité permanent de la justice et des questions juridiques demande au gouvernement de déposer une réponse globale dans les 120 jours suivant le dépôt du présent rapport à la Chambre des communes.

NOTES

(1) La liste des témoins qui ont comparu devant le Sous-comité se trouve à l'Annexe «A».

(2) Le premier ordinateur, l'ENIAC (intégrateur et calculateur électronique numérique), a vu le jour en 1946 à l'Université de Pennsylvanie. Pour de plus amples détails, voir S. Sokolik, «The Computer Crime—The Need for Deterrent Legislation», *Computer/Law Journal*, vol. II, no 2, printemps 1980, pp. 353-385 (p. 354).

(3) *Security World*, janvier 1982, p. 28.

(4) Témoignage présenté par M. Peter Ward, de Peat, Marwick and Partners. Voir les procès-verbaux et témoignages du Sous-comité de la Chambre des communes sur les infractions relatives aux ordinateurs, le 27 avril 1983, 4:18.

(5) S.R.C. 1970, c. C-34.

(6) *R. c. Christensen et al.* (1978), 26 *Chitty's Law Journal*, p. 348 (Cour suprême de l'Alberta, Division de première instance).

(7) *McLaughlin c. R.* (1979), 12 C.R. (3d) 391 (Cour d'appel de l'Alberta); et *Sa Majesté la Reine c. McLaughlin* (1980) 2 R.C.S. 331 (Cour suprême du Canada).

(8) Cette enquête de la Sûreté provinciale de l'Ontario, intitulée «Sondage sur la criminalité et la sécurité informatiques», a été présentée par le Surintendant G.W. Allen, de la Section des délits commerciaux de la G.R.C., qui a comparu devant le Sous-comité le 17 mars 1983.

(9) Témoignage présenté par M. Peter Ward, de Peat, Marwick and Partners. Voir les *Procès-verbaux et témoignages* du Sous-comité de la Chambre des communes sur les infractions relatives aux ordinateurs, le 27 avril 1983, 4:6.

(10) *R. c. Stewart* (1982), 68 C.C.C. (2d) 305.

(11) S.R.C. 1970, c. C-30.

(12) *R. c. McMullen* (1979), 100 D.L.R. (3d) 671.

(13) *R. c. Bell and Bruce* (1982), 65 C.C.C. (2d) 377.

(14) *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, S.Q. 1982, c. 30.

(15) S.C. 1982, c. 111 et S.R.C. 1970, c. I-5 modifié, respectivement.

(16) Voir les *Procès-verbaux et témoignages* du Sous-comité de la Chambre des communes sur les infractions relatives aux ordinateurs, le 19 mai 1983, 10:7.

(17) Voir les *Procès-verbaux et témoignages* du Sous-comité de la Chambre des communes sur les infractions relatives aux ordinateurs, le 25 mai 1983, 12:11.

Annexe «A»

TÉMOINS QUI ONT COMPARU DEVANT LE SOUS-COMITÉ

	Date de la comparution
Du ministère de la Justice	
M. Norman Hill, chef de projet, Projet vol et fraude	Le 17 mars 1983
M. Neville Avison, chef, Recherche et statistiques	Le 17 mars 1983
De la Gendarmerie royale du Canada	
Surintendant George W. Allen, Section des délits commerciaux	Le 23 mars 1983
De Cerberus Computer Services Inc.	
M. James Finch, Toronto	Le 23 mars 1983
M. Collin C. Rous, Toronto	Le 23 mars 1983
De l'Association canadienne des fabricants d'équipement de bureau	
M. John Reid, président du Comité de la législation (ACFEB)	Le avril 19 1983
M. Howard Kaufman, vice-président, Xérox	Le avril 19 1983
M. John Dean, conseiller juridique principal, IBM	Le avril 19 1983
De Peat, Marwick and Partners	
M. Peter Ward, Toronto	Le avril 27 1983
De l'Université Western, Ontario	
M. John Palmer, professeur, London (Ontario)	Le 3 mai 1983
M. David H. Flaherty, professeur, London (Ontario)	Le 3 mai 1983
De Landspan International of Canada Ltd.	
M. Peter J. Lawrence, président-directeur	Le 10 mai 1983
M. J. Ian Henderson, vice-président et avocat-conseil général, Ottawa (Ontario)	Le 10 mai 1983
M. Morvin Gentleman, Conseil national de recherches	Le 11 mai 1983
M. Frank Spitzer, expert-conseil, Toronto	Le 11 mai 1983
M. Dave M. Conway, directeur, Protection des ressources, Mitel Corporation, Kanata (Ontario)	Le 17 mai 1983
M. Tony J. Juliani, professeur, Département de Criminologie, Université d'Ottawa	Le 17 mai 1983

M. Grant Hammond, professeur et avocat, Centre d'études juridiques, Université de l'Alberta, Edmonton (Alberta)	Le 18 mai 1983
Me George E. Fisk, avocat, «Gowling and Henderson Barristers», Ottawa (Ontario)	Le 18 mai 1983
M. Paul C. Boire Sr., président, l'Association canadienne des entreprises de services en informatique (CADAPSO), Ottawa	Le 19 mai 1983
M. D.W. Kay, directeur de district, Datacrown Inc., Ottawa	Le 19 mai 1983
Du ministère de la Consommation et des Corporations:	
M. Tony Butler, conseiller principal en matière de politiques	Le 24 mai 1983
M. Bruce Cauchman, conseiller en matière de politiques	Le 24 mai 1983
De l'Association canadienne de l'informatique, Toronto	
Mme Sally Woodhead, présidente, Groupe spécial d'intérêt sur la sécurité informatique	Le 25 mai 1983
De l'Association des banquiers canadiens	
M. R.M. MacIntosh, président	Le 26 mai 1983
M. E. Jestin, superviseur, Vérification et évaluation interne, La Banque de Nouvelle-Écosse	Le 26 mai 1983
Mlle Pat Learmonth, coordinatrice des communications	Le 26 mai 1983
De l'Association canadienne des consommateurs	
Mlle Christine Bisanz, directrice suppléante, Politique et activités	Le 31 mai 1983
Mlle Christine Elliott, membre, section Ontario	Le 31 mai 1983
De Gaston, Snow and Ely Bartlett, Palo Alto, Californie	
Mme Susan H. Nycum, avocate	Le 1er juin 1983
De l'Association du barreau canadien	
Me Yves Fortier, président	Le 8 juin 1983
Me Bernard E. Blanchard, directeur général	Le 8 juin 1983
Me Judith Kingston et	Le 8 juin 1983
Me Charles W. MacIntosh, c.r., du Comité permanent du droit, des sciences et de la technologie	Le 8 juin 1983
Me Stephen Georgas, avocat, Toronto	Le 9 juin 1983
Du ministère de la Justice:	
M. E.A. Tollefson, coordonnateur, Révision du Code criminel	Le 9 juin 1983
M. Norman Hill, chef de projet, Projet vol et fraude	Le 9 juin 1983

Annexe «B»

BIBLIOGRAPHIE SOMMAIRE

Cette «Bibliographie sommaire» contient la liste des principaux articles et ouvrages consultés pendant les travaux et lors de la rédaction du rapport. La Bibliothèque du Parlement a dressé une liste plus complète de plus de 300 titres de revues et d'articles savants. On peut se procurer cette liste en s'adressant au greffier du Sous-comité de la Chambre des communes sur les infractions relatives aux ordinateurs.

Becker, J., «Rifkin, A Documentary History», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 471-720.

Becker, J., «The Trial of a Computer Crime», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 441-456.

États-Unis, ministère de la Justice, Bureau of Justice Statistics, Criminal Justice Resource Manual. Computer Crime, Washington, 1979.

Hammond, G. R., «Quantum Physics, Econometric Models and Property Rights to Information», *McGill Law Journal*, vol. 27, 1981, 47-72.

Ingraham, D., «On Charging Computer Crime», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 429-439.

Kling, R., «Computer Abuse and Computer Crime as Organization Activities», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 403-427.

Krieger, M., «Current and Proposed Computer Crime Legislation», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 721-771.

Palmer, J. et Resendes, R., Le droit d'auteur et les ordinateurs, Approvisionnements et Services Canada, 1982.

Parker, D.B., «Computer Abuse Research Update», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 329-352.

Schjolberg, S., «Computer/Assisted Crime in Scandinavia», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 457-469.

Simkin, M., «Is Computer Crime Important?», *Journal of Systems Management*, mai 1982, 34-38.

Sokolik, S.L., «Computer Crime - The Need for Deterrent Legislation», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 353-383.

Taber, J.K., «A Survey of Computer Crime Studies», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 275-327.

Volgyes, M., «The Investigation, Prosecution and Prevention of Computer Crime: A State-of-the-Art Review», *Computer/Law Journal*, vol. II, no 2, printemps 1980, 385-402.

Watkins, P., «Computer Crime: Separating the Myth From the Reality», *CA* Magazine, jan. 1981.

Whiteside, T., «The Annals of Crime», *New Yorker*, le 22 août 1977 (1ère partie); le 29 août 1977 (2e partie).

Un exemplaire des Procès-verbaux et témoignages du Sous-comité sur les infractions relatives aux ordinateurs (fascicules nos 1 à 17 inclusivement et 18 qui comprend le présent rapport) et un exemplaire des Procès-verbaux et témoignages du Comité permanent de la justice et des questions juridiques (fascicules nos 117, 119, 131 et 132) sont déposés.

Respectueusement soumis,

Le président,
CLAUDE-ANDRÉ LACHANCE

PROCÈS-VERBAL

LE MARDI 14 JUIN 1983

(20)

[*Texte*]

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à huis clos, à 15h40, sous la présidence de M. Ken Robinson (*Etobicoke—Lakeshore*), président suppléant.

Membre du Sous-comité présent: M^me^ Hervieux-Payette.

Membres substituts désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^me^ M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^er^ mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1*).

Le Sous-comité entreprend l'étude du projet de rapport sur les infractions relatives aux ordinateurs.

A 17h30, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

LE JEUDI 16 JUIN 1983

(21)

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à huis clos, à 17h05, sous la présidence de M^me^ Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^me^ Hervieux-Payette.

Aussi présent: M^me^ M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^er^ mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n° 1*).

Le Sous-comité reprend l'étude du projet de rapport sur les infractions relatives aux ordinateurs.

A 18h14, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le Sous-comité sur les infractions relatives aux ordinateurs se réunit aujourd'hui à huis clos, à 10h01, sous la présidence de M^me^ Céline Hervieux-Payette, président.

Membre du Sous-comité présent: M^me^ Hervieux-Payette.

Membres substituts désignés présents: MM. Beatty et Robinson (*Etobicoke—Lakeshore*).

Aussi présent: M^me^ M. Hébert, recherchiste, Service de la recherche, Bibliothèque du Parlement.

Le Sous-comité reprend l'étude de son ordre de renvoi du mardi 1^er^ mars 1983. (*Voir procès-verbal du mardi 15 mars 1983, fascicule n°1*).

Le Sous-comité reprend l'étude du projet de rapport sur les infractions relatives aux ordinateurs.

Sur motion de M. Robinson (*Etobicoke—Lakeshore*), le Troisième Rapport du Sous-comité sur les infractions relatives aux ordinateurs, tel que modifié, est adopté.

Il est ordonné,—Que le Président fasse rapport du Rapport au Comité permanent de la justice et des questions juridiques.

Il est convenu,—Que le Rapport soit imprimé en forme tête-bêche avec une couverture spéciale de couleur verte.

Sur motion de M. Beatty, il est ordonné,—Que soient imprimées 2000 copies additionnelles du fascicule n° 18 des procès-verbaux et témoignages du Sous-comité.

A 12h00, le Sous-comité suspend ses travaux jusqu'à nouvelle convocation du président.

Le greffier du Sous-comité
Pierre de Champlain