

TÉLÉCOMMISSION



Étude 5 b)

**Rapport de la conférence sur les ordinateurs
Vie privée et liberté d'information**

QUEEN
HE
7815
.A5214
no. 5b

Ministère des Communications

Queen
HE
7815
, AS214
no. 5b

78
S102.5
G35
5 (b) f
c.1

TÉLÉCOMMISSION

Étude 5b)

Industry Canada
Library Queen
AOUT 27 1998
AUG 27 1998
Industrie Canada
Bibliothèque Queen

RAPPORT DE LA CONFÉRENCE SUR LES ORDINATEURS

Vie Privée et liberté d'information

Université Queen's
Du 21 au 24 mai 1970

~~COMMUNICATIONS CANADA
NOV 23 1972
LIBRARY - BIBLIOTHÈQUE~~

© Droits de la Couronne réservés

En vente chez Information Canada à Ottawa,
et dans les librairies d'Information Canada:

HALIFAX
1735, rue Barrington

MONTRÉAL
1182 ouest, rue Ste-Catherine

OTTAWA
171, rue Slater

TORONTO
221, rue Yonge

WINNIPEG
393, avenue Portage

VANCOUVER
657, rue Granville

ou chez votre libraire.

Prix \$2.00

N° de catalogue Co 41-1/5BF

Prix sujet à changement sans avis préalable

Information Canada
Ottawa, 1972

Ce rapport a été rédigé, pour le compte du ministère des Communications, par un groupe de travail composé de représentants de divers organismes, institutions et entreprises. Il ne reflète donc pas nécessairement les vues du Ministère ni celles du gouvernement fédéral et n'engage en aucune façon leur politique.

Le lecteur devra considérer ce rapport comme un document de travail dont la terminologie n'est pas nécessairement celle qu'ont adoptée les auteurs d'autres études de la Télécommission.

"LES ORDINATEURS: VIE PRIVÉE ET LIBERTÉ D'INFORMATION"

	<u>Page</u>
PRÉFACE	1
INTRODUCTION	4
Chapitre I - Vie privée: Concepts sociaux et juridiques	10
1. Vie privée et dignité	10
2. Définitions de la vie privée	13
3. Evaluation du concept de la vie privée	14
4. Statut juridique de la vie privée et de la liberté d'information	20
Chapitre II - Information et systèmes d'information	24
1. Quelques systèmes d'information: pratiques actuelles et problèmes de politiques	26
2. Classification des systèmes d'information	33
Chapitre III - Ordinateurs et systèmes d'information	38
1. Comment les ordinateurs peuvent empoisonner la vie privée	39
2. Possibilité financière et technique de systèmes d'information par ordinateur	42
3. Sécurité des systèmes d'information par ordinateur	47
Chapitre IV - Mesures suggérées	52
1. Droit à la vie privée	54
2. Comment empêcher les abus dans l'utilisation des systèmes d'informatique	60
3. Moyens d'action	69
4. Note concernant la compétence législative	70
5. Considérations internationales	71
6. Conclusion	71
Annexes	
Annexe A Recommandations	73
Annexe B Ateliers	79
Annexe C Participants	83

Préface

L'effet possible des ordinateurs sur les particuliers, leurs valeurs et leurs droits, et notamment l'intrusion dans leur vie privée par les systèmes d'informatique sont des sujets de préoccupation universelle, comme on a pu le voir lors des longues audiences qui ont eu lieu au Congrès américain au sujet du projet d'une banque nationale de données, dans la Résolution N° 1028 de la vingt-sixième session de l'Assemblée Générale des Nations Unies concernant les droits de l'homme et les développements scientifiques et technologiques, et aussi dans les études entreprises aux Etats-Unis, en Grande-Bretagne, en Allemagne de l'Ouest, en Suède et au Danemark. Au Canada, les quatre organismes mentionnés ci-dessous ont organisé, au début de 1970, une conférence sur le même sujet:

- le ministère des Communications
- le ministère de la Justice
- la Société canadienne d'informatique
- l'Université Queen's

Le présent rapport résume les travaux de cette conférence, qui a eu lieu à l'Université Queen's (Kingston, Ontario) du 21 au 24 mai 1970.

Deux comités ont été formés, l'un pour l'organisation et l'autre pour l'élaboration du programme de la conférence. Reconnaisant la double nécessité de respecter la vie privée des gens et de préserver la liberté d'accès à l'information, les membres de ces comités ont choisi pour la conférence le titre suivant: "Les ordinateurs: vie privée et liberté d'information" et ils ont établi les objectifs suivants:

- a) définir, après examen et discussions, les problèmes de vie privée et de droit d'accès qui découlent du fonctionnement des systèmes d'informatique et des banques de données;
- b) identifier les difficultés susceptibles de se produire dans l'application de la technologie des ordinateurs à la compilation, à la mémorisation et à l'extraction de l'information;
- c) proposer des directives pour la protection de la vie privée et de l'accès à l'information dans la technologie de demain;

- d) recueillir les opinions qualifiées d'un groupe représentatif de spécialistes qui s'occupent de la conception, du fonctionnement ou de l'utilisation des systèmes d'informatique et des banques de données en ce qui concerne le respect de la vie privée et le droit d'accès à l'information.

Trois préoccupations majeures ont présidé à la mise sur pied de la conférence.

- 1) S'efforcer d'obtenir une gamme complète de points de vue. Pour y parvenir, il fallait choisir avec soin les sujets, les conférenciers et les participants.
- 2) S'efforcer de dépasser le niveau habituel de discussion sur ce thème, et s'attaquer à des problèmes bien spécifiques et formuler des propositions détaillées. On y parviendrait:
 - en limitant le nombre des participants et en choisissant des personnes qui s'occupent déjà de ces questions ou des personnes appelées à s'en occuper dans un proche avenir;
 - en distribuant à l'avance aux participants de la documentation pertinente afin qu'ils soient préparés et qu'ils partagent des connaissances communes;
 - en organisant des ateliers multi-disciplinaires avec des petits groupes de personnes afin que les échanges de vues soient spontanés;
 - en veillant à ce que des mesures adéquates soient prises pour la distribution des documents et la rédaction des procès-verbaux. Cela suppose qu'il fallait distribuer les textes écrits des exposés, que les rapporteurs des ateliers devaient préparer des résumés et que le rapport final donne une image cohérente de la conférence toute entière;
 - en fournissant la documentation voulue pour certaines propositions concernant les ordinateurs et les banques de données, et en enregistrant dans quelle mesure on était d'accord ou non sur ces propositions.
- 3) S'efforcer de placer le thème de la conférence dans un contexte canadien. On y parviendrait:

- en veillant à ce que les documents de base comportent des textes relatifs aux lois et aux pratiques canadiennes;
- en n'oubliant pas que la responsabilité du choix des conférenciers, des interlocuteurs et des participants revient conjointement aux autorités fédérales et provinciales;
- en prévoyant les textes dans les deux langues officielles et en fournissant un service d'interprétation simultanée lors des discussions.

Comme le dit l'introduction, la conférence a suscité un consensus étonnant en ce qui concerne la nature et la portée des problèmes d'intrusion dans la vie privée des gens causés par le développement rapide des systèmes d'informatique, et en ce qui concerne les solutions envisagées pour résoudre ces problèmes. L'élaboration de leurs solutions dépendra des études recommandées par la conférence. Leur application subséquente sera la responsabilité des autorités compétentes, gouvernementales ou autres.

L'original du rapport final de la conférence a été rédigé en anglais par M. Ian Rodger, du Financial Post. Selon le comité des programmes, ce document reflète fidèlement à la fois l'étendue du consensus atteint et le degré de désaccord manifesté. Enfin, nous devons remercier l'Université Queen's pour l'excellence des dispositions matérielles, qui ont largement contribué au succès de cette conférence.

Le Président de la conférence,

R.J. Gwyn

Le Président du Comité du programme,

C.C. Gotlieb

Introduction

La tenue d'une conférence visant à explorer les effets de la technologie sur le droit à la vie privée et sur la liberté d'accès à l'information, comme l'a fait remarquer M. John Turner, ministre de la Justice, "n'est pas sans présenter une grande importance, ni sans revêtir une certaine valeur historique". Cependant, M. Turner ajoutait:

"Il ne s'agit pas tellement d'une occasion de nous féliciter nous-mêmes, mais plutôt d'une occasion de faire notre propre autocritique, car les problèmes de vie privée et d'accès à l'information posés par la cybernétique ne sont pas nouveaux pour nous. En fait, le problème générique du droit à la vie privée, ou des menaces d'intrusion dans la privée, fait partie de la tradition intellectuelle et des enquêtes jurisprudentielles américaines depuis 1890.

S'il est vrai que Louis Brandeis, qui devait plus tard devenir sous-ministre de la Justice aux Etats-Unis, fut le co-auteur en 1890 d'un article sur le droit à la vie privée, ce n'est qu'au cours des années 1960 que le problème a pris vraiment de l'ampleur aux Etats-Unis et ailleurs. Ce serait une tâche énorme, et peut-être inutile, que de vouloir retracer les raisons qui expliqueraient soit le manque d'intérêt qui a existé dans le passé en ce qui concerne le droit à la vie privée, soit le développement rapide d'un grand intérêt pour cette question au cours des récentes années. Comme la pollution, le droit à la vie privée est un "problème" dont nous avons soudainement pris conscience.

L'inquiétude actuelle concernant la vie privée face à l'ordinateur a probablement été amorcée par le projet de 1965 du Conseil de recherche sur les sciences sociales des Etats-Unis, qui voulait que le Bureau du Budget établisse un "centre national de données" pour compiler et fournir des renseignements concernant les citoyens par suite de la pénétration grandissante du gouvernement dans les domaines complexes de la pauvreté, de la santé, de la rénovation urbaine et de l'éducation. Cette proposition, soumise à un sous-comité du Congrès, a donné lieu aux célèbres audiences de 1966 sur les "ordinateurs et la vie privée" qui se sont tenues sous la présidence du représentant Cornelius Gallagher. La réaction des politiciens et du public à cette proposition a été immédiate, bruyante et presque entièrement négative.

Depuis lors, des quantités d'articles, de livres, d'études juridiques et de propositions législatives ont vu le jour.

Aux Etats-Unis, une importante étude organisée par l'Académie nationale des sciences sera terminée en juin 1971, et le Congrès continue à être aux prises avec cette question. En Grande-Bretagne, le Parlement a mis sur pied une commission d'enquête qui a pour mission d'étudier le même problème. En France, le Conseil d'Etat a été chargé au début de 1970 d'étudier les problèmes juridiques de l'informatique ainsi que les défis posés par les ordinateurs aux libertés individuelles. En Suède, une commission royale a été établie en 1966 pour élaborer des projets de loi en ce qui concerne la protection de la vie privée en général contre l'intrusion des dispositifs techniques et scientifiques. Une étude semblable est actuellement en cours au Danemark.

Aux Etats-Unis, deux livres importants, Privacy and Freedom, par Alan F. Westin, professeur à l'Université Columbia et The Death of Privacy, par Jerry Rosenberg, ont été publiés respectivement en 1967 et 1969. Le Professeur Westin publiera prochainement un second livre sur la vie privée, de même que M. Arthur Miller, professeur à l'Université du Michigan.

L'Organisation de Coopération et de Développement Economiques (OCDE) et les Nations Unies ont fait de la protection de la vie privée un important sujet d'étude.

Le gouvernement provincial de la Colombie-Britannique a mis en vigueur une loi assurant le droit à la vie privée. A l'Assemblée législative de l'Ontario, un projet de loi privé vise à restreindre l'activité des "banques de données". Au Québec, on a proposé un amendement au Code civil afin que soit protégée la vie privée des personnes. Plusieurs propositions ont été faites par le Professeur Ed Ryan, dans un étude intitulée Protection of Privacy in Ontario, qu'il avait entreprise pour le compte de l'Ontario Law Reform Commission.

Un fait surprenant se dégage de toutes ces analyses et de cette préoccupation face au problème de la vie privée: la "vie privée" n'a jamais fait l'objet d'une définition objective; on l'a souvent décrite et chacun a une version subjective de ce qu'il considère être sa vie privée et sa propriété personnelle. L'une des définitions les plus succinctes, mais non des plus complètes, a été énoncée par la Conférence nordique de 1964 sur le droit à la vie privée: "Le droit de pouvoir mener en paix sa propre vie, avec un minimum d'immixtion."

Le Professeur Westin, par exemple, considère que la vie privée est un besoin humain fondamental apparenté à l'exigence territoriale que les hommes de sciences ont découverte chez les animaux. Dans Privacy and Freedom, il a écrit: "Les études faites sur les animaux montrent que virtuellement toutes les bêtes ont besoin d'un isolement individuel temporaire ou d'une intimité en petits groupes, ce sont là deux aspects très

importants de la vie privée." La mesure dans laquelle la vie privée a été reconnue et respectée a cependant beaucoup varié d'une société à l'autre. Pour prendre deux exemples opposés, il faut rappeler que la langue arabe n'a pas de mot pour "vie privée", mais que les sociétés anglo-saxonnes considèrent que le charbonnier est roi dans sa maison.

En considérant les sociétés anglo-saxonnes dans une perspective historique, on est amené à une conclusion inattendue, à savoir que l'homme moyen a probablement plus d'intimité aujourd'hui qu'il n'en a jamais eu auparavant. De nos jours, la plupart d'entre nous ne vivent qu'avec une ou deux autres personnes, dans l'un de ces énormes et impersonnels ensembles urbains. Nos grands-parents vivaient le plus souvent dans de petits villages où l'anonymat, donc la vie privée, étaient impossibles. Tout le monde connaissait les péchés de ses voisins.

Par ailleurs, il faut préciser que les ordinateurs n'ont pas créé de toute pièce le danger de l'intrusion dans la vie des gens. Les gouvernements, les entreprises commerciales et la police ont toujours eu des dossiers importants qui contenaient des renseignements sur un grand nombre de personnes bien avant la venue des ordinateurs numériques. L'informatique a simplement rendu beaucoup plus efficaces la compilation, la manipulation et la diffusion des données.

Voici ce qu'a dit à ce sujet le ministre des Communications, M. Eric Kierans, lors de l'ouverture de la conférence tenue à l'Université Queen's:

"Cette conférence est une étape, et rien qu'une étape, dans l'exploration de l'invasion possible de la vie privée qui pourrait être amenée par le développement rapide des systèmes d'informatique et des banques de données. Il est évident que ce développement va donner lieu à des inconvénients de nature sociale qu'il y a lieu d'examiner à la lumière des avantages économiques et autres que l'on peut attendre des ordinateurs. C'est précisément le genre de problèmes que nous devons étudier et résoudre, si nous voulons éviter une pollution technologique globale qui accompagnerait notre pollution industrielle. Cette pollution technologique pourrait avoir comme conséquence de changer complètement notre comportement social et nos priorités afin de nous adapter aux exigences mécaniques des machines."

Environ 150 hommes d'affaires, avocats, informaticiens, économistes, éducateurs, sociologues et simples particuliers ont participé aux travaux de cette conférence. Certains participants sont arrivés, semble-t-il, convaincus que les ordinateurs ne créaient aucun problème pour la vie privée des citoyens et ils

espéraient même que la conférence pourrait tout simplement régler la question une fois pour toutes. Quelques participants croyaient que la conférence visait à mettre en vigueur une nouvelle série de mesures restrictives qui donneraient un pouvoir accru aux autorités gouvernementales. D'autres encore semblaient tellement désireux de faire adopter des lois révolutionnaires qu'ils n'avaient pas tenu compte des dommages qui pourraient être infligés au système économique et aux institutions établies au pays.

Ces divergences de vues prouvent que les organisateurs de la conférence avaient bien fait leur travail, et que, comme l'a dit le président: "La conférence elle-même, dans la mesure où la faiblesse humaine le permet, est représentative de l'industrie, des utilisateurs et des membres intéressés des universités, du barreau et du gouvernement. On peut également avancer que ces divers groupes sont proportionnellement représentés à la conférence."

La conférence a débuté par une table ronde générale dont le sujet était "Vie privée et liberté comme concepts sociaux et juridiques." La conférence a comporté cinq autres tables rondes entrecoupées de quatre ateliers. Les titres des autres tables rondes étaient les suivants:

- b) Banques de données: technologie et pratiques actuelles.
- c) Banques de données: orientation de leur développement à la suite des besoins et de la technologie.
- d) Objectifs à établir pour assurer le respect de la vie privée et la liberté d'information dans les banques de données.
- e) Moyens légaux et réglementaires qui permettront d'atteindre les objectifs établis.
- f) Moyens professionnels et techniques qui permettront d'atteindre les objectifs établis.

Pour les ateliers, les participants ont été répartis en groupes de 12 à 16 afin de favoriser des discussions libres sur les points soulevés lors des tables rondes. Chaque atelier a soumis le samedi soir après la dernière réunion des ateliers un rapport contenant ses vues et ses recommandations. Le secrétariat de la conférence a étudié les rapports des ateliers et en a extrait un rapport final qui a été soumis à l'approbation de la session plénière de la conférence. Des exemplaires des rapports d'atelier ont également été remis aux participants pour

vérification. Le texte approuvé du rapport de la conférence figure à l'Annexe A.

On a également expliqué à la session plénière qu'au lieu de publier un procès-verbal textuel de la conférence, on rédigerait un rapport qui serait distribué à tous les participants. On s'efforcerait dans ce rapport de noter toutes les données et opinions importantes et intéressantes qui sont ressorties des mémoires écrits, des tables rondes et des périodes des questions et réponses qui ont suivi les tables rondes et les ateliers.² Et surtout, on s'efforcerait dans le rapport de présenter toute cette documentation sous une forme cohérente et bien compréhensible.

Le rapport ci-après est le résultat de ces efforts. Les données qu'il contient ne suivent pas forcément l'ordre chronologique des discussions mais tâche plutôt de grouper les commentaires et discussions qui ont trait à un même sujet. En voulant rendre le rapport complet, les rédacteurs ont peut-être donné l'impression qu'il y avait de grandes différences dans les points de vue des participants. C'est effectivement ce qui s'est produit. Cependant, pour la plupart des questions débattues, on a pu discerner le début d'un consensus qui était marqué soit par le défaut d'arguments soit par une synthèse apparente à la suite de longues discussions. La plupart des participants ont été vraiment étonnés à la fin de la conférence de voir qu'on avait obtenu un tel consensus.

Le présent rapport est divisé en quatre chapitres.

Le chapitre I traite des problèmes liés à la définition de la vie privée comme concept social et juridique. Cette définition est fondamentale lorsqu'il s'agit d'évaluer les pratiques actuelles susceptibles de provoquer des intrusions dans la vie privée. Elle est encore plus importante pour ceux qui cherchent à prévoir les développements technologiques de l'avenir qui pourraient violer la vie privée dans une mesure encore plus grande. Par exemple, c'est un fait connu que les gouvernements, les commissions scolaires, les médecins, la police et d'autres personnes ou organismes se livrent à des activités qui les amènent, à différents degrés, à pénétrer dans la vie privée des particuliers. Il est cependant impossible de savoir si ces activités sont acceptables ou non tant que n'aura pas été établie une définition générale de la "vie privée." De plus, il se pourrait fort bien que les nouvelles technologies mises au service des autorités gouvernementales, des médecins, etc. arrivent à changer la nature de leurs activités au point qu'elles envahissent littéralement la vie privée des gens. Cette définition générale de la vie privée est également nécessaire pour déterminer les aspects justes et injustes d'une telle situation. A la fin du chapitre I, se trouve un résumé de

l'historique du concept de vie privée tel qu'il a été traité dans les lois.

Le chapitre II concerne l'information. Il fait la synthèse des diverses notions relatives à la puissance de l'information et des moyens par lesquels le développement des "systèmes d'information" influe sur cette puissance. A titre d'exemple, on décrit dans ce chapitre le fonctionnement de quelques systèmes d'information. Enfin, des suggestions sont faites quant à la façon dont pourraient être classés les systèmes d'information.

Le chapitre III passe en revue la question de l'effet des ordinateurs sur les systèmes d'information. On y explique comment les ordinateurs pourraient, pour le meilleur ou pour le pire, modifier les systèmes d'information. La possibilité technique et économique du développement de très grands systèmes d'information fait aussi l'objet d'un compte rendu.

Finalement, le chapitre IV contient les diverses recommandations de la conférence et leur justification.

Chapitre I

Vie privée: Concepts sociaux et juridiques

"La vie privée est peut-être l'une des choses, comme la beauté, la vérité et la liberté, qui n'existent que dans la pensée des gens". Cette remarque de M. Leon Katz, membre du Conseil des sciences du Canada et professeur de physique à l'Université de la Saskatchewan, semble résumer toutes les tentatives frustrantes qui ont été faites par les délégués pour définir la vie privée. La question de la vie privée en tant que concept social et juridique a été examinée de près par la première table ronde de la conférence, mais pas suffisamment semble-t-il puisqu'elle est revenue à la surface à plusieurs reprises au cours des ateliers et durant les périodes de questions. De nombreux délégués étaient d'avis qu'il était inutile de parler d'autre chose tant qu'on n'aurait pas réglé cette question. Le rapport de la conférence ne fait qu'énumérer les principales écoles de pensées.

Plusieurs ateliers ont parlé de la nécessité de résoudre la notion de la vie privée comme concept juridique ou même d'élaborer une philosophie de la vie privée. Quelques ateliers ont estimé que ce travail n'était pas possible, à moins de le confier à un comité spécial. D'autres ont jugé que le concept de la vie privée varie selon les circonstances historiques et sociales, et que sa définition revient aux tribunaux. D'autres encore sont arrivés à la conclusion que le droit à la vie privée devrait être énoncé dans les lois, et qu'il devrait être conforme à la Déclaration universelle des droits de l'homme.³

Avec le recul, on peut voir dans les nombreux mémoires et débats sur cette question que la recherche d'une définition de la vie privée n'était pas la bonne formule pour aborder le problème. En partant du principe que la vie privée, quelle que soit sa nature ou sa définition, est vitale pour la dignité des personnes, et qu'elle peut même lui être synonyme, le problème consiste alors plutôt à préciser quelles sont les actions qui offensent la dignité d'une personne, d'un groupe ou d'un pays, et ensuite à prendre des mesures pour y remédier. Pour commencer, cependant, il y a lieu d'établir la validité du principe voulant que la vie privée est indispensable à la dignité de l'homme.

1. Vie privée et dignité

"En tant que société évoluée, nous avons toujours fait des intrusions dans la vie privée. Nous avons toujours forcé les pauvres, les jeunes et les mères célibataires à mettre leur âme à nu; mais ce n'est que récemment que la classe moyenne s'est préoccupée du droit à la vie

privée, car les membres de cette classe courent maintenant le risque de voir leur vie intime violée."

Thomas L. McPhail, Université Loyola

L'un des exemples les plus frappants de la façon dont la qualité et même la nature de l'existence d'une personne peuvent être changées par des intrusions dans son intimité a été fourni par M. Tim Reid, député au Parlement ontarien, participant à la conférence et auteur d'un projet de loi concernant les banques de données et la vie privée qu'il a déposé à la Législature ontarienne en 1969. L'exemple donné concernait l'utilisation qu'on avait faite de renseignements recueillis au sujet d'élèves du cours secondaire.

M. Reid a fait remarquer que les étudiants, sachant que des rapports complets sont rédigés sur eux par les professeurs et les administrateurs, sont sous une tension extraordinaire afin de se conformer aux exigences.* Il a mentionné le cas d'un jeune président de classe à qui il avait envoyé une lettre aux soins du bureau du principal. La lettre en question fut ouverte au bureau du principal avant d'être remise à l'étudiant. Ce dernier se trouvait face à un dilemme: "si je fais des histoires, quelqu'un inscrira à mon dossier qu'on ne peut se fier à moi et que je ne suis qu'un fauteur de troubles." M. Reid a ensuite appliqué cet exemple à l'ensemble de la société.

"L'étudiant qui sait que l'on recueille des renseignements à son sujet, et qui souhaite avoir une bonne réputation pour pouvoir aller à l'université et obtenir éventuellement une bonne situation, est comme le père de famille conscient de la surveillance que des agences d'investigation exercent maintenant sur lui. Les gens ne font que commencer à se rendre compte qu'on recueille beaucoup de renseignements à leur sujet. Les réactions sont de deux sortes. Il y a ceux qui se défendent parce qu'ils n'ont rien à craindre et il y a ceux, les plus nombreux, qui se disent qu'il vaut mieux attendre encore dix ans, jusqu'à ce que les enfants aient grandi, la période pendant laquelle les besoins de la famille réclament qu'on soit solvable; en attendant, ils adoptent une attitude conformiste et évitent de s'engager dans une lutte pour se protéger contre ces pernicieuses intrusions dans leur vie privée."

M. John Turner, ministre de la Justice, a, en réponse à une question, distillé l'essence même de ce problème. "Le droit de n'être pas d'accord est un droit très difficile à maintenir s'il n'y a pas de possibilité de discuter sans crainte d'être entendu. Toute politique démocratique dépend d'un grand nombre de relations confidentielles, d'appuis obtenus dans le privé, etc."

Un autre exemple de la façon dont le sentiment d'être surveillé peut modifier le comportement d'une personne a été donné par M. Claude-Armand Sheppard, avocat de Montréal et participant à la table ronde "Concepts de la vie privée." Il a décrit le cas hypothétique d'un homme marié qui, à l'insu de sa femme, est un habitué d'un bar fréquenté par les homosexuels. Cet homme sait pertinemment que la police fait souvent des descentes dans les bars de ce genre et qu'elle peut y avoir remarqué sa présence. Si cet homme était accusé d'avoir commis un délit n'ayant aucun rapport avec le fait qu'il fréquente le bar susmentionné, ne se pourrait-il pas, demandait M. Sheppard, qu'il hésite à se défendre avec ténacité de peur que la police ne fasse mention de ses activités dans le bar, ce qui le mettrait en très mauvaise posture vis-à-vis de sa femme et de sa famille?

C'est probablement à ce genre de réaction à la surveillance que devait penser M.A.E. Gotlieb, sous-ministre des Communications, lorsqu'il a déclaré:

"Il se peut que la personne en vienne à se sentir tellement épiée dans une société dominée par l'information, qu'elle change de comportement et préfère agir comme ceux qui l'entourent et ne pas se faire remarquer."

Le résultat, selon M. Gotlieb, "serait une société atrophiee dont les membres ne feraient preuve d'aucune initiative et d'aucune volonté d'innover."

La surveillance qui réussit à recueillir les données qu'une personne considère comme confidentielles détruit la dignité de cette personne. Le maintien du sens de la dignité selon M. Turner, ministre de la Justice, revêt une importance cruciale dans toute société démocratique.

"L'érosion de la vie privée est le commencement de la fin pour la liberté. En effet, la vie privée est le fondement du principe de l'autonomie, qui est le centre vital de la dignité humaine. Le droit à la vie privée non seulement atteint le fond de notre être en tant que personnes humaines mais aussi le fond de notre être en tant que société ou Etat. Tout Etat qui dégrade ses citoyens se dégrade lui-même. Une société qui fait fi de la vie privée de ses membres fait aussi fi d'elle-même."

Il est cependant extrêmement difficile de définir exactement ce que les gens considèrent comme privé et personnel; quelles sont les invasions de la vie privée qui feront tort à la dignité d'une personne et quelles sont celles qui passeront inaperçues. Si ces invasions inacceptable peuvent être

découvertes, il y aura un problème juridique également difficile à résoudre pour ce qui est de permettre qu'elles se produisent.

"La congestion est la seule chose qui sauvera la vie privée. Aujourd'hui, l'endroit le plus isolé qui soit est dans sa voiture au milieu d'un embouteillage."

-Gordon Thompson, Bell Canada-Northern Electric Research Ltd.

2. Définitions de la vie privée

Le simple fait de demander ce que signifie la vie privée indique clairement qu'un important changement s'est fait, et continue probablement de se faire, dans la conception que l'on a de sa définition. En d'autres termes, les gens se posent cette question parce qu'ils voient autour d'eux des preuves que les activités qu'ils considéraient comme privées autrefois ne le sont plus aujourd'hui, et que des choses qu'ils considéraient comme publiques sont maintenant de nature privée. Il n'est pas difficile de citer des exemples. Un participant a dit que lorsqu'il était jeune, son père n'aurait jamais dit à personne combien il gagnait. Ce renseignement est maintenant public. Par contre, certains aspects de la vie communautaire qui étaient autrefois connus à tous sont maintenant de nature privée. Combien parmi les locataires de grands immeubles d'aujourd'hui connaissent même seulement de vue leurs voisins?

M. R.F. Linden, spécialiste de l'informatique au ministère fédéral de l'Industrie et du Commerce, a prétendu que le concept de la vie privée varie non seulement avec le temps et avec les générations mais qu'il change d'un pays, d'une région et d'un groupe social à l'autre. Il a dit qu'en Allemagne, par exemple, les gens sont sidérés par l'ampelur des systèmes nord-américains d'information sur la solvabilité, et qu'ils considèrent ces systèmes comme des violation flagrantes de la vie privée des gens. Les Allemands pourtant ne voient pas d'inconvénients à prévenir la police chaque fois qu'ils changent de résidence alors que cela ne plairait probablement pas aux gens d'ici. Les Hollandais, toujours d'après M. Linden, n'auront pas de numéros d'assurance sociale ou d'autres preuves d'identité semblable pendant encore au moins trois générations pour la raison suivante: lorsque les Allemands ont occupé la Hollande durant la Deuxième Guerre mondiale, la Gestapo a donné un numéro à chaque Hollandais. C'est pourquoi ils considèrent les numéros d'assurance sociale comme une menace à la vie privée. Les Danois acceptent que leur gouvernement tienne des dossiers à jour sur tous les citoyens mais ils refusent que les données soient mises en ordinateur. Durant la guerre, semble-t-il, lorsque les Danois voulaient cacher quelqu'un, ils pouvaient subtiliser son dossier. Une telle subtilisation serait très difficile si les données étaient enregistrées dans la mémoire d'un ordinateur.

Le commun dénominateur de tous ces exemples est la personne qui, à un moment donné, est confrontée par une situation qui peut compromettre son sens de la dignité, et même sa propre sécurité, parce que l'on s'est immiscé dans un domaine qu'elle considère comme étant de sa vie privée. Le point important est que cette évaluation se situe dans l'esprit de celui que en est victime. Elle est complètement subjective. Comme pour toutes les images mentales, celles de la vie privée et celles de la vie personnelle évoluent aussi avec le temps, l'expérience et la culture. En somme, le concept de la vie privée est de nature dynamique. Il ne répond à aucune définition, sinon en des termes qui sont eux-mêmes dynamiques.

3. Évaluation du concept de la vie privée

Si le concept de la vie privée est de nature dynamique, le problème qui se pose est de définir ce qu'il est à un moment donné pour un groupe social donné. Car ce n'est que lorsque tout le monde est d'accord sur la notion de la vie privée qu'une société peut prendre des mesures juridiques contre ceux qui empiètent sur les droits établis en matière d'intimité. Plusieurs suggestions ont été faites durant la conférence quant aux moyens d'évaluer les notions de la vie privée d'un groupe donné. Tous les moyens proposés semblaient être basés sur une tension qui existe dans chaque cas où la vie privée est en jeu. Cette tension existe entre ceux qui veulent que les renseignements de nature personnelle restent confidentiels et ceux qui souhaitent que ces renseignements soient plus ou moins publics. Il semble y avoir une très grande variété de situations types dans lesquelles prend place cette bataille entre ce qui est privé et ce qui est public. Ces situations types pourraient être groupées en plusieurs catégories.

La conférence semble avoir retenu deux catégories principales:

- a) celle où la personne désire garder pour elle certains renseignements de nature personnelle alors qu'un organisme privé ou public cherche à recueillir ces renseignements pour un nombre de fins quelconques;
- b) celle où la personne désire obtenir des renseignements que des organismes gouvernementaux ou privés ne veulent pas dévoiler.

Naturellement ces deux situations peuvent se produire simultanément. Par exemple, un bureau de crédit peut chercher à obtenir et à garder des renseignements concernant une personne, renseignements que cette dernière n'aurait pas été disposée à fournir. De plus, le bureau de crédit peut refuser de faire connaître à cette personne le contenu du dossier ainsi établi.

Dans presque tous les cas, en outre, il semble que l'individu doive lutter contre de puissantes institutions comme les organismes du gouvernement, les établissements de recherche ou les grosses entreprises. La conciliation des droits et des intérêts légitimes des deux parties n'est pas une tâche facile.

Le Professeur Thomas McPhail, sociologue de l'Université Loyola à Montréal, et participant à la table ronde sur le respect de la vie privée dans les banques de données, a fourni un exemple important du dilemme des chercheurs en sciences sociales.

"Il n'y a aucun doute que les chercheurs en sciences sociales violent la vie privée des gens. Il suffit pour s'en convaincre de consulter les études désormais classiques de Kinsey ou les études plus contemporaines de Johnson & Masters publiées dans ces deux livres: Human Sexual Response et Sex Behavior in the Human Animal. En tant que chercheur en sciences sociales, je suis très conscient qu'une législation canadienne est absolument nécessaire pour protéger les citoyens contre les invasions brutales et peu démocratiques faites dans la vie privée par les autorités gouvernementales et militaires et par des organismes publics ou privés qui se soucient peu de la dignité humaine. Cependant, en tant que chercheur en sciences sociales, je suis également conscient du fait qu'un excès de zèle pour protéger tout le monde contre tout risquerait de mettre fin à la recherche en sciences sociales dans de nombreux domaines excessivement importants... Le droit de recueillir des données, particulièrement dans des domaines aussi délicats que ceux de la famille, de la religion, du revenu, de l'illégitimité, de l'éducation, de l'alcoolisme, du divorce, et de l'avortement, est essentiel pour certaines recherches en sciences sociales."

Des opinions semblables ont été exprimées par des planificateurs du gouvernement, des statisticiens et des hommes d'affaires qui font des études de marché. Leur argument est qu'ils ne recueillent des renseignements que pour détecter des tendances, et qu'ils ne cherchent nullement à apparenter les données qu'ils obtiennent aux noms de personnes particulières. Ils promettent non seulement de protéger la dignité des gens, mais aussi de faire des études qui leur profiteront d'une façon ou d'une autre.

Aussi impressionnants qu'ils soient, ces arguments semblent faire suite à un fait accompli. En d'autres termes, les planificateurs, les statisticiens et les autres collectionneurs de données semblent ne pas s'être préoccupés de savoir si les gens aiment ou non faire l'objet de recherches. Ayant tout simplement énoncé l'importance et la légitimité de leurs

fonctions, ils les ont exercées sans trop se préoccuper des plaintes de ceux qui faisaient l'objet de ces recherches. Comme l'a dit M. M.T. Pearson, directeur général de l'Associated Credit Bureaus of Canada: "On ne demande jamais aux consommateurs ce qu'ils pensent." Pour évaluer les sentiments d'un groupe social concernant la vie privée dans des situations comme celle-ci, il faudrait, semble-t-il, déterminer dans quelle mesure les membres de ce groupe sont prêts à accepter les sondages de diverses agences, même si l'anonymat est respecté ou que ces sondages sont fait pour le bien d'une personne ou d'une collectivité. A quel moment, par exemple, ces personnes décident-elles qu'il y va de leur intérêt de ne pas divulguer de renseignements à leur sujet?

M. A.E. Gotlieb, du ministère des Communications, a déterminé comme suit le sens d'une décision de ce genre prise par une personne: "C'est le droit de débrancher, c'est-à-dire de ne pas communiquer". Selon M. Gotlieb, l'un des principes fondamentaux de notre société:

"est le respect de la liberté des gens, une liberté qui peut s'exprimer par un choix entre la communication et l'isolement. Chacun devrait être libre de ne pas se procurer de renseignements. Mais cela n'est qu'un aspect du droit à l'information. Ce droit comprend également le droit de ne pas communiquer involontairement, c'est-à-dire le droit d'une personne de limiter l'emploi que l'on peut faire des renseignements qui ont été recueillis à son sujet."

Un autre groupe de collectionneurs de données, en tête duquel figurent les bureaux de crédit et les bureaux de personnel, ne voient que partiellement l'identité des personnes, ce qu'ils justifient en disant que leurs systèmes d'information sont indispensables pour le fonctionnement efficace du système économique. M. Pearson a soutenu dans son mémoire que "les Canadiens ont un meilleur niveau de vie que jamais parce qu'ils sont dans une société qui est axée sur le crédit..." "Sans les bureaux de crédit, il est probable que les entreprises commerciales hésiteraient à faire crédit sans de longues et coûteuses enquêtes. On refuserait de faire crédit à de nombreuses personnes méritantes, particulièrement les salariés moyens, à cause de renseignements insuffisants. Par ailleurs, les délais feraient perdre des ventes et réduiraient le volume des affaires." Bien que cet argument soit certainement juste, il semble bien encore qu'on n'a pas demandé l'opinion des gens à ce sujet. La question clé serait la suivante: à quel moment une personne estime-t-elle que le fonctionnement efficace du système économique empiète sur sa dignité? Quel degré d'efficacité est-elle prête à perdre afin d'être astreinte à moins d'enquêtes?

D'autres groupes de collectionneurs de données, comme les médecins, les avocats, les organismes policiers, etc.

recueillent aussi des données personnelles pour différentes raisons, et ils en font usage avec plus ou moins de discrétion. Dans chaque cas, c'est un défi pour la personne qui fait l'objet de l'enquête. Accepte-t-elle que ces organismes recueillent et utilisent des renseignements la concernant ou se sent-elle compromise de quelque façon que ce soit si ces renseignements sont divulgués? On dirait que personne ne s'est préoccupé de faire le jour sur ces questions. Leurs réponses sont pourtant essentielles si on veut connaître la mesure dans laquelle les personnes désirent qu'on respecte leur vie privée afin de préserver leur dignité.

L'autre catégorie de confrontations sur l'accès à la vie privé se retrouve dans des situations où une personne souhaite se procurer des renseignements que d'aucuns voudraient ne pas divulguer. M. A.E. Gotlieb a décrit ainsi dans son mémoire ce genre de situation:

"C'est le droit de communiquer, ou, en fait, le droit d'être branché. Dans la société dominée par l'information vers laquelle nous nous dirigeons, personne ne devrait avoir à rester en dehors des circuits automatisés d'information. Les désavantages en seraient trop grands, et le fossé créé pour les personnes non informées deviendrait infranchissable par d'autres moyens."

Comme on l'a fait remarquer durant la conférence, ce désir est actuellement concrétisé dans la personne qui veut obtenir des renseignements détenus par les gouvernements. Généralement, les gouvernements ont tendance à garder pour eux les renseignements relatifs à leurs activités, même lorsqu'ils n'ont aucune justification pour le faire. Comme l'a dit M. John Turner, ministre de la Justice, "C'est une tendance qu'ont les gouvernements d'empiéter sur les droits des citoyens sous le sceau du secret. En d'autres termes, le secret des gouvernements est parfois légitimé comme étant un de ses droits, mais ce droit peut parfois s'opposer au droit qu'a le public d'être informé."

L'impression qu'il y avait des abus dans ce domaine était très générale durant la conférence. Dix ateliers étaient d'avis qu'il fallait protéger la liberté d'accès à l'information, et on peut lire ce qui suit dans le rapport de la conférence: "ce besoin a été considéré comme particulièrement important en ce qui concerne l'information gouvernementale." De nombreux participants ont dit que ce droit d'accès à l'information devrait s'étendre à d'autres domaines, en particulier pour permettre aux gens d'inspecter leurs dossiers dans les bureaux de crédit, etc. afin de faire corriger les erreurs. Certains voudraient aller plus loin, d'autres moins loin. On a cependant reconnu le danger que des institutions exploitent certains renseignements confidentiels au détriment des personnes concernées.

Ce danger découle du concept de l'information comme moyen de contrôle, à savoir que la possession exclusive de certains types de renseignements confère à celui qui les a un certain pouvoir. L'utilisation de renseignements compromettants contre une personne afin de la faire chanter en est un exemple. D'autres situations, à la fois plus subtiles et plus effrayantes dans leurs conséquences possibles, ont été mentionnées au début du présent chapitre. Un danger connexe, pour paraphraser M. Allan Gotlieb, est le fossé qui va en s'élargissant entre le petit groupe de gens qui recueillent et manipulent les renseignements et les masses qui sont manipulées, particulièrement lorsqu'elles sont conscientes qu'elles le sont ou qu'elles peuvent l'être.⁶ Si ce fossé s'élargissait trop, on aboutirait à une société paranoïaque et intellectuellement atrophiée. Le développement de techniques électroniques avancées qui permettent de recueillir, de mémoriser et de diffuser des données laisse prévoir que ce danger est très réel. M. Hugh Lawford, professeur de droit à l'Université Queen's, a décrit l'une des nombreuses façons dont les ordinateurs peuvent élargir ce fossé.

"Il est tout à fait possible d'établir un système d'information sous contrôle gouvernemental dans lequel seulement certaines personnes autorisées auraient accès aux seuls documents qu'elles auraient le droit de consulter. Etant donné que les ordinateurs permettent l'affichage de l'information sur des écrans de télévision placés dans les bureaux des personnes autorisées, point n'est besoin de faire des copies permanentes de documents. Du fait que l'ordinateur peut enregistrer les noms de toutes les personnes autorisées ayant consulté un document, la responsabilité dans le cas où des données appartenant au gouvernement seraient révélées sans autorisation peut être assez facilement établie. Un seul système pourrait desservir tout un ministère, et peut-être même tout un gouvernement, au moyen de dossiers électroniques centralisés. Ces dossiers ne nécessitent pas une armée d'employés, de messagers et de bibliothécaires, et le nombre de fonctionnaires chargés de la protection de l'information peut être très réduit."

Ces dangers, à savoir que les institutions possèdent des renseignements personnels de nature très délicate qui leur permettraient de manipuler les personnes concernées, et que ces renseignements puissent devenir la propriété d'un nombre de plus en plus réduit de personnes, peuvent être atténués d'au moins deux façons. L'une serait de forcer les manipulateurs éventuels à mettre leurs données à la disposition de tout le monde, ce qui leur enlèverait toute possibilité de soumettre des gens au chantage ou de les intimider; l'autre consisterait à défendre totalement aux manipulateurs éventuels d'accumuler des données.

Il est évident que dans certaines situations, peut-être pour des raisons de sécurité nationale, il faut recueillir des renseignements et les garder secrets. Mais M. Turner a été le premier à admettre que ces situations sont rares et qu'elles sont généralement acceptées du public. Il peut y avoir d'autres situations où le public préférerait que les renseignements soient gardés secrets; d'autres encore où le public admet que les renseignements doivent être confidentiels mais où il réclame le droit de vérifier leur exactitude, et d'autres enfin où le public s'en moque peut-être. Mais, encore une fois, personne ne semble savoir ce que le public pense ou ce qu'il veut.

C'est alors qu'on est tenté de suggérer que les organismes qui recueillent des renseignements mettent fin à leur activité et fassent de sérieux sondages d'opinions. Ce faisant, ils apprendraient jusqu'à quel point le public est prêt à fournir des renseignements et dans quelle mesure il désire avoir accès aux renseignements recueillis par d'autres. Ce serait un pas dans la bonne direction, mais il y aurait naturellement des dangers à éviter. En 1968, The Associated Credit Bureaus of Canada (ACBA) a fait une étude qui constitue une des rares initiatives dans ce sens. M. Pearson, directeur général de l'ACBA, a signalé à la suite de cette étude que "le public est peu conscient du rôle des bureaux de crédit, et que son intérêt pour la façon dont sont menées les enquêtes sur la solvabilité est presque nul."

Sans vouloir critiquer les efforts de l'ACBA, on peut dire que cet exemple fait ressortir le grave problème qui se pose chaque fois que l'on cherche à sonder les sentiments du public sur de tels sujets. Dans des sondages de cette nature, on pourrait chercher à définir la tolérance maximale des gens aux intrusions faites dans leur vie privée et à l'intimidation. Beaucoup "d'histoires d'horreur" contées à la conférence indiquent clairement que beaucoup de gens se sont déjà tranquillement et humblement soumis à ces intrusions dans leur vie privée. D'un autre côté, une tâche encore plus difficile consisterait à définir les limites qu'il y aurait lieu de ne pas dépasser dans ces intrusions pour que les gens ne perdent pas le sens de leur dignité. En somme, comment amener les gens à dire avec précision comment rétablir une partie de leur dignité qui leur est enlevée petit à petit.

Un problème connexe est celui de décider quelles mesures devraient être prises pour que des renseignements précis puissent être acquis. Un atelier de la conférence en est arrivé à l'étonnante conclusion que toute décision relative à la question de savoir si les renseignements devraient être gardés secrets ou remis aux autorités compétentes devrait être fondée sur le principe du "plus grand bien pour le plus grand nombre de gens". Cela est étonnant car une douzaine de participants ont en fait convenu que le principe du respect des droits des minorités,

principe crucial dans les décisions relatives à la vie privée, devrait être ignoré.

4. Statut juridique de la vie privée et de la liberté d'information

"Il existe des lois qui protègent, et ont protégé pendant de nombreuses années, certains aspects de la vie privée des citoyens. Je pense en particulier aux lois relatives à la propriété, aux lois qui reconnaissent certains droits humains fondamentaux, aux lois sur la diffamation et la calomnie, aux lois qui confèrent un statut confidentiel à l'information échangée, par exemple, entre un médecin et son patient et aux lois relatives à l'interception des conversations téléphoniques. En pratique cependant, ces lois n'assurent pas une protection suffisante de la vie privée. Au Canada, par exemple, l'emploi des émetteurs radio miniaturisés et des "mouchards" électroniques, n'est pas réglementé... On reproche souvent aux lois d'être statiques et en retard sur la technologie. Cette critique est probablement justifiée. Si cela devait se continuer dans l'avenir, les conséquences pourraient être encore plus graves qu'elles ne l'ont été dans le passé."

M. A.E. Gotlieb
(extrait d'un mémoire).

Les lois mentionnées par M. Gotlieb non seulement ne protègent pas adéquatement la vie privée, mais dans la plupart des cas, ces lois ne sont même pas destinées à la protéger. Les lois visant la diffamation, par exemple, n'ont qu'un seul but: protéger les gens contre le libelle immérité. Elles n'offrent aucune protection contre la diffusion de renseignements embarrassants mais vrais. En Grande-Bretagne, la loi qui interdit le branchement de lignes d'écoute n'est pas fondée sur le principe de la protection de la vie privée. Le branchement est interdit car on le considère comme un vol d'électricité, qui appartient au ministère des Postes.

"Le droit à la vie privée n'est guère reconnu et protégé dans nos lois." Cette déclaration a été faite par le Professeur Douglas A. Schmeiser, de l'Université de la Saskatchewan, et président d'une table ronde sur les questions juridiques. M. Schmeiser a ajouté: "on ne le trouve pas dans la Déclaration canadienne des droits de l'homme; on ne le trouve pas dans les déclarations correspondantes des provinces; il est expressément exclu des procédures judiciaires, de la plupart des communications professionnelles et des méthodes policières modernes." M. Claude Armand Sheppard a été du même avis: "En droit, ce concept de la vie privée est relativement nouveau. Il

existe dans la jurisprudence canadienne, mais sa reconnaissance a généralement été plus implicite qu'explicite. On s'en est occupé de façon fragmentaire et un peu au hasard."

M. Sheppard a noté une reconnaissance symbolique du principe de la garantie du secret du courrier dans la Loi sur les postes, dans divers statuts fédéraux et provinciaux interdisant le brouillage ou l'écoute des conversations téléphoniques. Il a également noté plusieurs dispositions du Code criminel, telles celles qui interdisent la surveillance des particuliers, des maisons d'habitation ou des lieux de travail, et celles qui exigent un mandat de perquisition pour qu'un agent puisse pénétrer dans des locaux privés. "A cet égard, il y a lieu de rappeler que les perquisitions doivent être effectuées de jour, à moins que le mandat ne les autorise la nuit."⁷

M. Sheppard a également fait remarquer que la loi québécoise ne contient aucune disposition spécifique concernant la vie privée, mais qu'un projet de loi sur les droits des citoyens contient un passage qui garantirait à chaque citoyen le droit de protéger sa dignité, son honneur, sa réputation et sa vie privée. Par ailleurs, il existe dans le Code civil de la province de Québec un précédent permettant d'employer les principes généraux de la responsabilité civile pour intenter une action en violation de la vie privée (voir note 7).

En somme, MM. Sheppard et Schmeiser semblent convenir avec le Professeur Westin que le principe de la vie privée a été reconnu dans le passé, mais que les lois sont bien en retard par rapport aux développements technologiques lorsqu'il s'agit d'incorporer des mesures destinées à protéger la vie privée.⁸

M. Hugh Lawford a prétendu de son côté que "le droit coutumier a été peu enclin à reconnaître le droit à la vie privée parce qu'un tel droit mettrait en danger celui, plus fondamental, de la liberté d'expression. Les restrictions que le droit coutumier a imposées à la liberté de communiquer des renseignements ont été interprétées à la lettre. Par exemple, les dédommagements accordés dans les lois pour les déclarations diffamatoires sont très limités. Même si quelqu'un parle de moi en termes qui me valent la haine ou le mépris publics, je ne peux pas poursuivre en justice mon détracteur s'il peut prouver que ce qu'il a dit est vrai." M. Lawford a également mentionné la tendance qu'ont les tribunaux de rejeter les demandes de ceux qui voudraient garder secrètes des catégories entières de renseignements pouvant servir de preuve.

Quelle que soit la perspective historique dans laquelle on observe le concept juridique de la vie privée, il est évident que ce concept n'a pas de fondement solide dans les lois canadiennes. Seule la Colombie-Britannique a des statuts particuliers en ce qui concerne la vie privée. Par ailleurs, peu

nombreuses sont les lois qui limitent l'activité des agences susceptibles de violer la vie privée des citoyens. Cependant, une étape importante a été franchie à la fin de 1970 lorsque M. John Turner, ministre de la Justice, a déposé à la Chambre des Communes un projet de loi visant à restreindre l'écoute électronique. Dans l'ensemble pourtant, peu de mesures ont été prises pour restreindre l'activité des collectionneurs de données, et on ne s'est guère penché sur les problèmes juridiques soulevés par l'apparition de "renseignements personnels" pouvant être employés comme agents ou outils d'invasion de la vie privée des gens.

Une autre lacune connexe des lois canadiennes est l'absence de lois qui prévoient ce que M. Turner appelle "le droit de savoir." Voici l'explication donnée par le ministre de la Justice:

"Il y a un autre aspect à considérer dans le droit à la vie privée, aspect qui n'a pas reçu toute l'attention qu'il mérite mais qui a pourtant une importance que l'on ne peut pas passer sous silence. Il s'agit de la tendance qu'ont les gouvernements à brimer les droits des citoyens en invoquant la nécessité du secret. En d'autres termes, le silence des gouvernements est parfois justifié en tant que droit pour un gouvernement d'avoir certains secrets, droit qui risque d'entraîner la négation du droit qu'a la public de savoir. Si la vie privée est le fondement de la démocratie, il n'en est pas moins vrai que le droit de savoir est fondamental à toute participation à cette démocratie. On ne peut pas s'attendre à ce que le public puisse dialoguer, et encore moins décider de façon intelligente, si on lui refuse l'accès aux renseignements qui rendraient possibles ce dialogue et cette prise de décision."

Le Professeur Hugh Lawford a expliqué en détail ce que l'absence d'un droit à l'information signifie pour un citoyen faisant affaire avec certains organismes fédéraux. "Le Canada", a-t-il déclaré, "n'a jamais promulgué de lois précises en ce qui concerne les documents publics et l'accès aux documents non publiés." Toujours selon M. Lawford, cette lacune existe tant en ce qui concerne les collections d'archives que les documents encore détenus par les ministères et les organismes du gouvernement.

"Il est même difficile de savoir qui a le pouvoir de donner la permission de consulter les documents du gouvernement. Il n'y a pas si longtemps, on prétendait encore que l'accès aux documents du gouvernement canadien était soumis à une "règle de 50 ans", à savoir que seuls les documents vieux de 50 ans et plus

pouvaient être mis à la disposition du public. Pourtant, il est difficile de trouver une justification légale quelconque pour la règle de 50 ans ou pour celle de 35 ans récemment annoncée par le premier ministre. Il existe certainement des dossiers vieux de plus de 50 ans que le gouvernement refuse de mettre à la disposition du public.

Les Canadiens n'arrivent pas à savoir de quelle loi dépend l'accès aux dossiers du gouvernement. Ils ne savent même pas si les ministères ont des fonctionnaires chargés de classer les dossiers au point de vue sécurité. En fait, on n'a jamais porté à l'attention du public la façon d'avoir accès aux dossiers du gouvernement, si toutefois cette façon de procéder existe."

Bien que MM. Turner et Lawford se concentrent sur l'idée que l'absence d'un "droit de savoir", particulièrement en ce qui concerne les documents du gouvernement, est dangereuse pour le mécanisme démocratique, il ne faudrait pas non plus oublier que cette lacune risque également de menacer la vie privée des citoyens. S'il en est ainsi, c'est que les fonctionnaires supérieurs qui possèdent des renseignements qu'ils ne veulent pas divulguer peuvent être en mesure de "manipuler" des personnes, des groupes, ou même la société toute entière. Comme l'a fait remarquer M. A.E. Ende de la Federal Communications Commission, et participant à la conférence: "Le danger véritable qui menace les particuliers provient des gouvernements qui recueillent des renseignements, les mettent en mémoire et les utilisent. Tout le monde peut être touché par l'opinion de gens puissants qui ont en leur possession des renseignements confidentiels."

Chapitre II

Information et systèmes d'information

A défaut d'autre chose, le chapitre précédent devrait avoir insinué que "l'information est le méchant". L'information est le "bien" qu'on voudrait sauvegarder pour soi tandis que les autres le convoitent. Dans certains cas, l'information sert aussi aux desseins des manipulateurs et des maîtres-chanteurs. Quand on traite de cette question, on en revient toujours à la notion de Bacon, à savoir que l'information confère la puissance... parfois. Certains renseignements n'ont aucune puissance, d'autres n'en ont que pour un instant, d'autres enfin ne sont puissants que dans certaines situations. Ainsi, M. R.J. Bouwman, conseiller juridique et secrétaire de la British Columbia Telephone Co., ne semble pas partager l'attitude alarmiste prise par de nombreuses personnes à cet égard.

"Je m'inquiète un peu au sujet de la peur dont tout le monde parle ici, c'est-à-dire la peur que tout le monde sache tout à votre sujet. Il m'importe peu qu'on me connaisse, qu'on connaisse le montant de mon compte en banque, etc. Je me suis demandé s'il est vrai qu'il existe une peur aussi terrible ou s'il s'agit d'une impression que nous sommes en train de faire naître graduellement chez les gens."

Ces remarques montrent bien que certains renseignements peuvent gagner ou perdre de la puissance selon les circonstances, et parfois de façon imprévisible. La puissance d'un certain fait peut être plus au moins grande selon que ce fait soit plus ou moins connu, elle peut dépendre du moment où il est rendu public ou d'un certain nombre d'autres circonstances.

La relation entre la puissance d'un renseignement et sa possibilité de faire du bien ou du mal aux gens varie également beaucoup. Parfois, l'information utile peut être puissante, parfois non. Quelquefois l'information susceptible de faire du mal peut être puissante, quelquefois non. Il arrive enfin que l'information ait de la puissance, qu'elle soit nuisible ou bénéfique.

Certains renseignements peuvent être puissants, qu'ils soient exacts ou non. On sait par exemple que les renseignements personnels qui figurent dans les fiches scolaires ou dans les dossiers des bureaux de crédit ont une influence énorme sur la vie des gens, quelle que soit leur exactitude. Pour un participant, l'aspect terrifiant de certains de ces renseignements est que les gens croient qu'ils sont vrais. Il a déclaré: "Nous vivons à une époque pseudo-scientifique, et on a tendance à surestimer les soi-disant données scientifiques." En fait, le peu d'importance accordé à l'exactitude dans des

situations comme celles-ci semble conférer une puissance supplémentaire à une information déjà très puissante. Cela découle, comme l'a fait remarquer M. Turner, de la peur qui se développe chez les citoyens et qui est amenée par leur "crainte que les renseignements ne soient pas exacts, que leur véracité et leurs sources n'aient pas été vérifiées, qu'ils soient teintés de préjugés, qu'on les utilise à des fins autres que celles pour lesquelles ils sont destinés, et qu'il n'existe pas de procédé de recours si ces renseignements sont utilisés sans qu'une personne le sache, donc sans son consentement."

Par contre, les gens ne sont nullement inquiets en ce qui concerne la véracité des renseignements qu'ils considèrent apparemment comme anodins. L'un des participants à la conférence a fait connaître les efforts faits par sa compagnie afin de vérifier l'exactitude de ses listes d'expédition. Lorsque la compagnie en question paie l'affranchissement de retour, 25% des personnes qui ont reçu un questionnaire de vérification y répondent. Lorsque la compagnie ne paie pas l'affranchissement de retour, seulement 8% des personnes répondent. En somme, d'après ce participant, "de toute façon 75% des gens s'en moquent éperdument."

Au milieu des ambiguïtés déconcertantes qui entourent l'information, au moins une de ses caractéristique est assez bien comprise, caractéristique qui a heureusement le plus retenu l'attention des participants. Il s'agit de la tendance qu'a l'information qui est déjà assez puissante de devenir de plus en plus puissante à mesure que grandissent les possibilités de mémorisation et de manipulation.

En d'autres termes, chaque invention, les hiéroglyphes, l'alphabet, le papier, la presse d'imprimerie, etc., ayant apporté à l'homme une plus grande capacité de mémorisation de l'information, elle a donné du même coup une puissance accrue à ceux qui la possédaient. Le développement plus récent de dispositifs mécaniques, électromécaniques et électroniques de traitement des données a rapidement augmenté cette puissance, comme on le verra dans un prochain chapitre.

Il est évident que les nouvelles méthodes et les nouveaux dispositifs pour mettre en mémoire ou extraire l'information n'ont pas été mis au point au hasard. C'était en vue de répondre aux besoins exprimés par ceux qui réalisaient, implicitement ou explicitement, l'avantage qu'il y avait à recueillir, mémoriser et manipuler certains types d'information. Il en résulte aujourd'hui une accumulation de données de tous genres qui sont en possession de personnes ou d'organismes plus ou moins importants. Certaines de ces données, qu'on les appelle systèmes de classement, systèmes d'information ou banques de données, sont gardées en ordinateur, d'autres sont enregistrées dans la mémoire humaine. Certaines, comme celles de l'annuaire

du téléphone, ont une grande diffusion; d'autres, comme les systèmes de la défense nationale, ont une diffusion extrêmement limitée.

Les pratiques et les problèmes des systèmes d'information qui ont le plus intéressé les participants à la conférence sont passés en revue dans le présent chapitre. On suggère des façons de classer les systèmes d'information afin de faire une distinction entre les systèmes conférant de la puissance et les systèmes inoffensifs. On ne cherche nullement dans le présent chapitre à séparer les systèmes d'information manuels des systèmes électroniques. Les problèmes étudiés ici s'appliquent quel que soit le moyen employé pour la mémorisation et la manipulation des données. L'effet de l'ordinateur sur les systèmes d'information sera étudié dans un prochain chapitre.

1. Quelques systèmes d'information: pratiques actuelles et problèmes de politiques

La conférence s'est penchée tout particulièrement sur les systèmes qui contiennent des renseignements sur des personnes. C'est pourquoi les discussions se sont concentrées sur les systèmes exploités par les agences de personnel et les bureaux de crédit et par les agences gouvernementales et paragouvernementales. Ces discussions se sont avérées fort utiles, car comme l'a fait remarquer le ministre de la Justice, nous ne connaissons pas grand chose au sujet de ces systèmes.

"Les systèmes d'information qui abondent dans les secteurs public et privé, et qui sont de plus en plus orientés vers des banques électroniques de données, savent beaucoup de choses à notre sujet alors que nous ne savons presque rien sur eux. Nous avons besoin aujourd'hui de renseignements concrets concernant les systèmes d'information et les banques de données, comme par exemple leur nombre, leur type, leur fonction, leur emplacement; quels sont les propriétaires de ces systèmes, tant du point de vue de leur nationalité que du point de vue de la participation du public; quel est le genre de données recueillies, mémorisées, extraites, transmises et divulguées; quelles ont été les mesures prises dans ces systèmes pour protéger les droits individuels et quelle est leur efficacité; quelles sont les tendances de la technologie de l'informatique et des banques de données pour le reste de la décennie?"

Trois conférenciers ont décrit lors de tables rondes les activités des bureaux de crédit, du Bureau fédéral de la Statistique et des commissions scolaires. Des discussions libres ont permis de mieux connaître les pratiques suivies par d'autres organismes qui recueillent des données.

M. M.T. Pearson, directeur général de l'Associated Credit Bureaus of Canada (153 membres), a parlé des méthodes et de la politique des bureaux de crédit. Il a souligné le rôle des bureaux de crédit dans notre société.

"Depuis 1951, le montant du crédit accordé au consommateur a quintuplé; il atteint actuellement les neuf milliards de dollars. Les 153 membres de l'ACBC fournissent chaque année plus de 5 millions de rapports de solvabilité, la plupart par téléphone, à plus de 40,000 abonnés."

M. Pearson a affirmé que cependant les bureaux de crédit ne prennent pas sur eux d'approuver ou de rejeter les demandes de crédit, qu'ils n'emploient pas d'enquêteurs pour sonder les faits et gestes des personnes, qu'ils ne constituent pas de dossiers secrets sur les personnes et qu'ils ne fournissent pas de rapports de solvabilité à tous ceux qui en font la demande.

Pour protéger les particuliers, l'ACBC exige la signature de contrats de service entre le bureau et les abonnés, dans lesquels il est certifié que "les enquêtes ne seront faites que pour des demandes de crédit et autres transactions commerciales légitimes, comme par exemple en vue d'établir la solvabilité actuelle et future." Lorsqu'un abonné ne respecte pas ces dispositions, on cesse de lui fournir le service. Les abonnés versent un montant annuel, plus une somme supplémentaire pour chaque rapport de solvabilité. Pour obtenir des renseignements, l'abonné doit s'identifier en rappelant le numéro de code spécifié dans le contrat.

"De plus, tout consommateur peut connaître le contenu de son dossier aux bureaux de crédit. Il lui suffit de demander un rendez-vous par téléphone. Lorsqu'il arrive au bureau de crédit, on lui demande de s'identifier. Ensuite, l'un des dirigeants du bureau de crédit examine avec lui le dossier qui le concerne."

M. Pearson a souligné le fait que les dossiers des bureaux de crédit ne contiennent que des données réelles. Il a dit que ces bureaux se sont rendu compte que les habitudes, les affiliations politiques, etc., d'une personne ne sont pas importants. "L'important est de savoir si la personne paye ou ne paye pas ses comptes. Il faut aussi dire que nous ne gardons pas les renseignements que nous ne pouvons pas vendre."

Ainsi, les dossiers des bureaux de crédit comprennent les renseignements suivants: nom de la personne, âge, résidence, résidences antérieures, état civil, enfants, employeur actuel, employeurs précédents, revenu estimé, façon dont la personne effectue généralement ses paiements, et comptes en souffrance.

"Les bureaux ne peuvent porter aux dossiers que les jugements et les actes judiciaires qui concernent le crédit aux consommateurs, les hypothèques mobilières enregistrées, les contrats de vente conditionnelle et les condamnations en vertu des statuts provinciaux ou pour des infractions criminelles."

"Les bureaux de crédit font état des faillites pendant 14 ans, et des comptes mis en collection, des jugements et des condamnations judiciaires pendant 7 ans."

M. Pearson a également présenté un tableau, établi à la suite d'une enquête effectuée par l'ACBC en 1968, et montrant le petit nombre de plaintes faites par les consommateurs aux bureaux de crédit (voir Tableau I).

Finalement, M. Pearson a fait remarquer "qu'aucun bureau de crédit au Canada n'utilise actuellement l'ordinateur, et qu'aucun n'a de projet concret de le faire." Pourtant, la maison mère de l'ACBC aux Etats-Unis et d'autres bureaux de crédit américains ont déjà mis leurs dossiers en mémoire sur ordinateur.

"Plusieurs secteurs de l'industrie canadienne qui desservent des marchés importants ont étudié la possibilité d'employer des ordinateurs, mais pour diverses raisons, comme le nombre, aucune décision n'a été prise jusqu'à présent", a ajouté M. Pearson.

Tableau I

Plaintes reçues et entrevues accordées en 1968 - Échantillonnage représentatif des
membres de l'ACBC

<u>Région</u>	<u>Nombre total de rapports en 1968</u>	<u>Nombre total de plaintes reçues</u>		<u>Nombre total de plaintes faites à la suite d'erreurs sur le rôle réel des bureaux*</u>		<u>Nombre total de plaintes à la suite d'erreur sur la personne</u>		<u>Nombre total de plaintes à la suite d'autres erreurs</u>	
		<u>Nombre</u>	<u>%</u>	<u>Nombre</u>	<u>%</u>	<u>Nombre</u>	<u>%</u>	<u>Nombre</u>	<u>%</u>
Maritimes	317,717	887	0.28	423	0.13	89	0.03	90	0.03
Québec	1,099,280	914	0.08	823	0.07	31	—	40	—
Ontario	1,662,587	3,114	0.19	2,015	0.12	47	—	69	—
Prairies	627,123	2,509	0.40	1,498	0.24	108	0.02	105	0.02
Colombie-Britannique	<u>570,285</u>	<u>2,081</u>	<u>0.36</u>	<u>1,156</u>	<u>0.20</u>	<u>95</u>	<u>0.02</u>	<u>44</u>	<u>0.01</u>
CANADA	4,276,992	9,505	0.22%	5,915	0.14%	370	0.01%	348	0.01%

* Dans presque tous ces cas, les consommateurs croyaient que les bureaux membres de l'ACBC approuvaient ou désapprouvaient les demandes de crédit.

"Cependant, la plupart des entreprises, en commençant par les plus importantes, admettent que l'utilisation de l'ordinateur deviendra indispensable et qu'elle dépend de considérations comme la quantité, la coût du matériel et le rendement des investissements. Dans ces conditions, il est raisonnable de supposer qu'une partie importante du secteur industriel au Canada aura recours aux ordinateurs dans 5 ou 10 ans, et que cela se produira plus tôt pour certains secteurs plus développés."

Les remarques de M. Pearson s'appliquent principalement à l'ACBC, qui groupe des agences qui recueillent des renseignements pour les garder en dossier. Les discussions qui ont suivi ont fait connaître les activités d'autres participants travaillant dans des entreprises où on recueille des renseignements au sujet des personnes. Le Professeur J.M. Carroll, de l'Université Western Ontario, a fait remarquer que "à toutes fins pratiques" il existait trois organisations du genre au Canada, les autres étant Dunn & Bradstreet, qui s'occupe surtout des maisons d'affaires et des gros investisseurs et The Retail Credit Co. of Canada. M. Carroll a souligné le fait que c'est surtout The Retail Credit Co. qui fait des enquêtes sur les particuliers pour le compte des compagnies d'assurance et autres entreprises semblables. Il a décrit ce genre d'activité comme de "l'espionnage d'alcôve et de bistro". Toutes ces agences, a-t-il ajouté, ont leur siège social aux Etats-Unis.

M. Carroll a aussi mis en doute la déclaration de M. Pearson selon laquelle un particulier peut consulter son dossier.

"Il a dit que n'importe quel consommateur a le droit de voir son dossier. Pourtant on aurait tort de croire qu'il suffit d'entrer dans un bureau de crédit, d'obtenir le document, de le tenir dans ses mains fébriles et d'examiner tout ce qu'on y dit à propos de soi-même. Cela ne se fait pas."

"Vous prenez rendez-vous", a poursuivi M. Carroll "pour consulter un dossier dans l'un des bureaux de crédit appartenant à l'entreprise de M. Pearson. Je ne sais pas si les autres bureaux vont même aussi loin. Ensuite, le gérant du bureau prend votre dossier en mains et vous dit: 'Monsieur Dupont, qu'est-ce qui vous inquiète au sujet de votre solvabilité?' En d'autres termes, il vous met sur la sellette et vous oblige à fournir des renseignements qui seront peut-être préjudiciables et qui ne sont peut-être pas encore contenus dans votre dossier. Je dis qu'il ne s'agit pas là du droit de consulter votre dossier. Tout ce qui existe, c'est le droit de se soumettre à un interrogatoire."

A cela M. Pearson a répondu: "Les renseignements sont codés pour garder leur caractère confidentiel. L'intéressé ne

comprendrait rien s'il voyait, par exemple, 'F - 100 - 1 - 69 - 1000 - \$60 - 800 - 01'. C'est pourquoi nous devons lui interpréter son dossier. Le point important est que ces dossiers contiennent les codes confidentiels que nos clients utilisent lorsqu'ils téléphonent. Si nous donnions un dossier à une personne, celle-ci pourrait relever le numéro de code et le communiquer à ses amis, qui à leur tour téléphoneraient au bureau pour avoir des renseignements de nature confidentielle".

Certaines des activités du gouvernement fédéral en matière de traitement des renseignements de nature personnelle ont été brièvement décrites par M. T.J. VanderNoot, du Bureau fédéral de la statistique.

Il a fait remarquer que la Loi sur la statistique garantit au citoyen qu'on ne peut utiliser contre lui les renseignements qu'il communique au Bureau fédéral de la statistique en vertu de ladite Loi.

La protection assurée par la Loi sur la statistique pour les renseignements personnels fournis comprend les trois grandes dispositions suivantes: (1) les questionnaires retournés dûment remplis par des personnes, des entreprises, etc., ne serviront qu'à des fins de statistiques, et leur contenu ne sera pas mis à la disposition du fisc ou d'autres autorités administratives et réglementaires quelles qu'elles soient; (2) les questionnaires remplis ne seront manipulés que par des employés assermentés du Bureau; (3) les données ainsi recueillies seront publiées sous une forme qui ne permettra pas d'identifier, sans autorisation préalable, des renseignements concernant un questionnaire en particulier.

En dépit des précautions prises pour assurer cette protection, M. VanderNoot a noté certaines difficultés, particulièrement en ce qui concerne la divulgation accidentelle.

Ceci se produit lorsque deux séries ou plus de données prises ensemble pourraient permettre de reconnaître celui qui a fourni les données, même si on n'a pas l'intention de l'identifier. Un exemple banal est la dissimulation d'une rubrique dans un tableau que l'on arrive quand même à déceler à partir des totaux partiels et des autres rubriques du tableau. Un exemple moins banal est la publication de certains totaux industriels par province et dans laquelle une rubrique contient les données de la seule entreprise qui oeuvre dans un secteur donné.

Le problème de la "divulgation accidentelle" illustre un point soulevé durant un atelier. Il n'est pas nécessaire que les

renseignements individuels qui figurent dans une banque de données portent le nom de l'intéressé pour être identifiables.

Il existe un autre danger implicite dans le fait que le Bureau fédéral de la statistique utilise des renseignements recueillis à des fins administratives par d'autres ministères et organismes gouvernementaux.

Il s'agit là d'une source de plus en plus riche de renseignements étant donné que les activités administratives des gouvernements modernes englobent des secteurs de plus en plus étendus. Cependant, le public craint que l'accumulation de données au sujet des particuliers au sein d'une seule agence ne permette le regroupement de renseignements provenant de diverses sources et ne donne ainsi naissance au dossier tant redouté qui a été décrit dans "1984".¹⁰

Une agence para-gouvernementale de collection de données qui a été étudiée est le système scolaire de l'Ontario. M. Tim Reid, député à la législature ontarienne, a déposé un projet de loi concernant les banques de données. Il a déclaré ce qui suit.

"Je redoutais de plus en plus ce qui se passait au sujet des dossiers des élèves dans les écoles primaires et secondaires, particulièrement lorsque sont apparus dans les années 1960 les bulletins sur lesquels les instituteurs et les professeurs étaient encouragés à écrire des remarques très subjectives sur le comportement social des élèves durant les classes et les activités para-scolaires, sur leurs fréquentations, leurs bonnes ou mauvaises habitudes, etc. En d'autres termes j'étais très inquiet du fait que des remarques très subjectives de nature psychologique étaient faites par des amateurs qui n'ont aucune formation en ce domaine."

Cette activité inquiétait M Reid, mais ce qui l'ennuyait encore plus est le fait que ces remarques étaient inscrites sur les fiches qui suivent les étudiants tout au long de leur carrière scolaire et universitaire. De plus M. Reid, appuyé par le Professeur John Carroll de l'Université Western Ontario, a soutenu que ces fiches sont souvent mises à la disposition de n'importe qui sans égard à leur caractère confidentiel.

Comme l'a dit M. Carroll, "Il arrive que les directeurs d'école à qui on demande des renseignements au sujet d'un élève s'empressent d'envoyer une photocopie de sa fiche à qui en fait la demande. Pourtant, il existe déjà des lois pour garantir le caractère confidentiel de ce document, la Loi sur les écoles secondaires je crois. Comme vous le voyez, nous parlons d'établir de nouvelles lois alors que nous n'avons même pas les

mécanismes nécessaires pour faire respecter les garanties déjà prévues dans les lois."

M. Reid a également fait mention de l'incident survenu à Toronto en juin 1969 lorsque la police a demandé et obtenu la fiche scolaire d'un garçon de 17 ans, ancien élève d'une école secondaire, qui devait servir de témoin à charge dans une affaire portée devant les tribunaux.

Une description intéressante des activités d'un autre groupe de collectionneurs de données a été présentée par M. Thomas McPhail, de l'Université Loyola. Il s'agit des spécialistes en sciences sociales. Prenant un exemple qu'il connaît bien, M. McPhail a parlé de la valeur de la recherche en sciences sociales, mais aussi des dangers latents que cette recherche fait courir aux particuliers et aux hommes de sciences qui s'y livrent. L'exemple concerne les recherches sur la marijuana.

"J'ai établi un questionnaire avec quelques collègues. La question 8 se lit ainsi: "Avez-vous déjà fumé de la marijuana?" Deux autres questions sont "Combien de fois?" et "Combien de fois vos amis en ont-ils fumé?" En tête du questionnaire on peut lire: "le présent questionnaire respecte l'anonymat et les réponses fournies ne seront publiées que groupées ensemble". Il s'agit là d'une recherche dans un domaine très délicat, mais je crois que les résultats obtenus nous permettent de mieux comprendre certains aspects du comportement humain qui jouent un rôle très important lorsqu'il s'agit de prendre des décisions. Par exemple, nous avons trouvé que 12% des étudiants de première année à l'université fument de la marijuana. En examinant ce qui se passe en deuxième, troisième et quatrième années, en maîtrise, puis au doctorat, le pourcentage des fumeurs de marijuana grimpe jusqu'à 80%. En d'autres termes, si on appliquait les lois fédérales telles qu'elles existent actuellement, la plus grande partie de l'élite de demain serait en prison. Je crois que ce genre de recherche est nécessaire, et pourtant je crains qu'on doive y mettre fin."

On a demandé à M. McPhail si la police pouvait saisir les données recueillies dans ce travail de recherche. Il a répondu: "elle pourrait peut-être m'y forcer par un quelconque moyen juridique; mais si je devenais au courant de leurs intentions, je m'empresserais de détruire ces données."

2. Classification des systèmes d'information

Naturellement, le but de la conférence n'était pas de faire le relevé des systèmes d'information exploités actuellement

au Canada. L'examen de quelques systèmes d'information a montré le genre de problèmes auxquels ces systèmes donnent lieu, même s'ils sont répartis par catégories. Un point à éclaircir, par exemple, est que l'expression "système d'information" décrit des choses aussi variées que l'annuaire du téléphone et les dossiers judiciaires de la Gendarmerie Royale du Canada, en passant par les catalogues du magasin Eaton, la liste confidentielle de clients d'une compagnie ou les dossiers des étudiants d'une commission scolaire. Toute tentative de les traiter comme un tout homogène conduira certainement à de curieux pièges. Par exemple, M. Hugh Lawford a montré que le libellé rigoureux du projet de loi du député Tim Reid au sujet des banques de données pourrait rendre illégale la publication des annuaires téléphoniques.¹¹

"Aux termes de ce projet de loi", a poursuivi M. Lawford, "je suppose que lorsqu'on édite un annuaire téléphonique, on établit un système de classement qui contient et garde des renseignements." M. Lawford a ensuite montré que l'annuaire téléphonique tombe sous les dispositions du paragraphe 3E du projet de loi de M. Reid, car il est vendu, sous celles du paragraphe 4, car il s'agit d'une banque de données qui contient des renseignements sur des personnes identifiables. En conclusion, M. Lawford a fait triomphalement savoir que si une personne découvre la moindre erreur ou donnée périmée dans un annuaire téléphonique, elle peut obliger la compagnie de téléphone à biffer l'information fautive ou à corriger l'erreur immédiatement, sinon une amende de \$10,000 lui sera imposée.

Un autre exemple de la façon dont une loi rédigée en termes trop généraux pourrait faire plus de mal que de bien, est la possibilité évoquée par plusieurs participants que les dossiers personnels d'une personne soient soumis à une réglementation, y compris l'examen des dossiers par les personnes qui y sont décrites, pour la raison que les "dossiers personnels" constituent des banques de données.

De tels exemples montrent qu'il faut trouver le moyen de classer les systèmes d'information et de donner des noms aux différentes catégories. D'une façon ou d'une autre, il y a lieu de séparer les systèmes potentiellement dangereux des systèmes inoffensifs, les systèmes à diffusion restreinte des systèmes à grande diffusion, etc.

Dans un rapport sur la classification, le Professeur C.C. Gotlieb de l'Université de Toronto, qui présidait le Comité du programme de la conférence, a suggéré de classer les systèmes d'information en fonction de trois caractéristiques: la source, l'étendue de la diffusion et la méthode qui autorise, si cela est permis, un particulier à examiner les renseignements consignés à son sujet.

En ce qui concerne les sources, M. Gotlieb a fait remarquer que les renseignements peuvent être fournis par les particuliers concernés, par des dossiers publics ou par d'autres sources, ces dernières étant définies par exclusion. Le seul problème ici est celui de définir "dossiers publics." Par exemple, est-ce que l'enregistrement des véhicules, les casiers judiciaires, les listes d'électeurs, etc. doivent être considérés comme des dossiers publics? M. Gotlieb a recommandé la prudence: "il serait nécessaire de bien réfléchir avant d'établir la classification, qui devrait être modifiée à la lumière de l'expérience acquise."

Dans la catégorie "inspection", M. Gotlieb a suggéré qu'on donne aux particuliers soit un droit automatique d'inspection (et alors on leur envoie périodiquement une copie des renseignements qui les concernent), soit le droit de demander la permission de voir ces renseignements. Une troisième possibilité consisterait à interdire tout accès à ces renseignements.

Quant à l'étendue de la diffusion des renseignements, le Professeur Gotlieb a proposé deux catégories, à savoir interne et externe, mais il a reconnu que ces catégories sont "extrêmement difficiles à définir."

"En général, la catégorie interne signifie que la distribution des renseignements est limitée à la compagnie ou à l'institution qui exploite le système d'information, à moins que le particulier concerné ne donne son autorisation explicite et dans chaque cas pour qu'on transmette les données ailleurs. Cependant, dans le cas du gouvernement fédéral et des gouvernements provinciaux, l'organisation est si vaste qu'il faudrait être encore beaucoup plus précis pour que le terme "interne" signifie quelque chose. Si on s'apercevait qu'il n'est pas possible de définir avec suffisamment de précision la diffusion interne, il faudrait peut-être envisager la diffusion du point de vue de renseignements spécifiques plutôt que du point de vue de l'ensemble des systèmes."

Le Professeur Gotlieb a alors donné quelques exemples de classifications pouvant être utilisées pour des systèmes connus d'information. Les dossiers des feuilles de paye comprennent des données en provenance "d'autres" sources (c'est-à-dire ne provenant pas de la personne elle-même ou des dossiers publics); elles n'ont qu'une diffusion interne et les intéressés peuvent probablement les consulter sur demande.

Les dossiers de police sont également constitués par des données en provenance "d'autres" sources mais il ont une diffusion externe et les intéressés ne peuvent pas les consulter.

Le Who's Who est un bottin constitué à partir de données fournies par les particuliers; il a une diffusion externe et les intéressés ont automatiquement le droit d'étudier leurs dossiers.

"La plupart de ces systèmes d'information sont employés depuis très longtemps. La réglementation pourrait commencer par l'identification des dossiers qui ont une diffusion externe mais que les particulier n'ont pas le droit de consulter. Aucune réglementation ne s'appliquerait aux autres systèmes. Cette façon d'agir encouragerait les exploitants de systèmes d'information à permettre l'inspection de leurs données par les intéressés et à restreindre, si possible, leur diffusion afin de ne pas être soumis à la réglementation."

Durant la conférence, M. Gotlieb a ajouté: "l'objectif véritable de ce mécanisme serait d'établir une vaste gamme de catégories de systèmes d'information qui ne seraient pas en général soumis à des règlements et ne nécessiteraient pas de licence spéciale. Le but de la classification des systèmes est de libérer virtuellement tous les systèmes d'information de la nécessité de détenir une licence, même lorsqu'ils contiennent des renseignements sur les personnes."

L'idée de la classification des systèmes d'information a frappé les esprits durant la conférence. Pourtant, elle s'est manifestée beaucoup plus comme une prise de conscience des différences qui existent entre les divers types d'information que comme une conception de ce que l'on pourrait faire au sujet de ces différences. Par exemple, un atelier en est arrivé à la conclusion qu'il y avait lieu de faire une distinction indispensable entre d'une part l'information subjective et qualitative, et d'autre part l'information objective et quantitative. Le même atelier a noté qu'il fallait également faire une distinction entre les renseignements recueillis à des fins de recherche et où les particuliers ne sont pas identifiés, et les renseignements personnels mémorisés et dont les intéressés sont identifiables. Un autre atelier, qui était pourtant favorable à la divulgation complète des renseignements qui sont entre les mains des gouvernements et des entreprises, a noté les restrictions suivantes:

"Les renseignements concernant les projets d'exploitation des compagnies, comme les investissements, les données susceptibles de renseigner les concurrents, etc. ne peuvent pas être divulgués sans faire tort aux compagnies concernées. D'autres renseignements, par exemple le parcours des autoroutes, ou ceux qui pourraient influencer les cours de la bourses ne devraient pas être divulgués."

Il est probable que la plupart de ces différences, sinon toutes, pourraient être résolues si les principes du systèmes de classification du Professeur Gotlieb étaient appliqués. M. Gotlieb a fait remarquer qu'il était en faveur du concept de la classification qu'il avait formulé mais qu'il ne devait pas nécessairement être appliqué à la lettre. Un domaine général de désaccord, cependant, pourrait concerner l'emploi que l'on fait des renseignements. M. Gotlieb, pour sa part, ne s'est pas montré intéressé à la façon dont l'information est employée. "Permettez moi de faire remarquer", a-t-il dit "que je n'essaie pas de classer l'information selon la façon dont elle est utilisée. Je crois que l'un des aspects des systèmes d'information est qu'ils ont toutes sortes d'usages auxquels on ne pense pas, et que de tenter de les découvrir tous ne serait probablement pas très utile."

Si on doit en croire les rapports des ateliers, le point de vue de M. Gotlieb était loin d'être partagé par tous. Trois ateliers ont conclu que les usages que l'on fait de l'information inquiètent beaucoup les gens, pourtant aucun atelier n'a expliqué pourquoi. Les exemples donnés comprenaient l'utilisation de renseignements sur la solvabilité dans le cas de demandes d'emploi, et la crainte que des renseignements donnés aux médecins, aux prêtres et aux avocats servent à d'autres fins. Un atelier s'est plaint de la vente des listes d'abonnés aux périodiques. Un autre atelier, cependant, en est arrivé à la conclusion que des gens qui donnent certains types de renseignements personnels se départissent du droit qu'ils ont de restreindre leur diffusion; on n'a pas donné d'exemple à ce sujet. M. Willis Ware, de la Rand Corporation, a dit lors d'un atelier que la peur que les renseignements soient utilisés par des tierces personnes peut découler du fait que "nous avons peur de l'avenir. Nous sommes victimes de nos émotions. Par exemple, nous nous inquiétons si on recueille des données sur notre état de santé, bien que ce soit pour notre bien. Pourquoi ne pas révéler l'indentité des personnes?" Mais M. Ware a également suggéré qu'on oblige les exploitants des banques de données à déclarer l'usage qu'ils font des renseignements qu'ils détiennent. (voir au Chapitre IV, la section 2 sur l'emploi abusif des systèmes d'information).

Chapitre III

Ordinateurs et systèmes d'information

"Je suis tout à fait prêt à reconnaître que les ordinateurs ont églament un droit à la vie privée."

-A.E. Gotlieb

"Un système électronique peut causer des injustices beaucoup plus efficacement et beaucoup plus rapidement que n'importe quel système manuel."

-Extrait d'un rapport d'atelier

Selon M. Robert Townsend, l'auteur de Up the Organization, "les ordinateurs sont de grosses et rapides machines à écrire et à compter qui sont coûteuses et bornées." C'est peut-être vrai, mais il est évident que cette définition passe sous silence les deux autres caractéristiques de l'ordinateur qui lui ont permis de révolutionner les systèmes d'information. Ces caractéristiques sont, d'un part, la capacité de mémoriser d'énormes quantités de données et, d'autre part, celle de pouvoir les extraire, les classer et les analyser à une vitesse foudroyante. M. John J. Deutsch, principal à l'Université Queen's et président de la table ronde sur les principes juridiques et sociaux de la vie privée, a déclaré ce qui suit:

"Autrefois, nous étions protégés par les restrictions inhérentes aux textes écrits. On pouvait certes accumuler beaucoup de renseignements mais cela finissait par prendre de la place. Il était difficile de retrouver, du moins rapidement, les renseignements que l'on cherchait. Tout cela a beaucoup contribué à protéger la vie privée des gens. Chercher un renseignement équivalait à chercher une aiguille dans une botte de foin. Aujourd'hui, on peut facilement retrouver cette aiguille."

Peut-être que le meilleur exemple du pouvoir qu'ont les ordinateurs de retrouver les aiguilles dans les bottes de foin a été fourni par M. T.J. VanderNoot, du Bureau fédéral de la statistique. Il a raconté qu'une entreprise américaine de mise en marché, la R.H. Donnelley Inc., avait accumulé des renseignements publics concernant des particuliers qui vivaient dans un certain quartier. Les sources d'information employées étaient les statistiques recueillies localement par le bureau de recensement, l'annuaire téléphonique et la liste des véhicules immatriculés achetée au bureaux des véhicules moteurs de l'état. Toutes ces données furent mises dans la mémoire d'un ordinateur et classées. A partir des résultats obtenus, cette entreprise a

pu découvrir beaucoup de choses au sujet des familles qui résidaient dans le quartier qui l'intéressait.

Et M. VanderNoot poursuivait: "J'aimerais faire remarquer que l'invasion de la vie privée n'est pas seulement une question de garder des dossiers ou de recueillir illégalement des renseignements. Mais à mesure que les sciences sociales elles-mêmes développent des méthodes plus élaborées, certains moyens parfaitement légaux peuvent être employés pour établir des dossiers au sujet d'une personne, ce qui constitue une intrusion dans la vie privée. Je demanderais aux avocats de nous expliquer comment une série d'actions parfaitement légales peut constituer finalement une violation de la vie privée."

Le hasard a voulu qu'un avocat, M. Allan Gotlieb, relève le défi, réponde à la question et montre qu'il y a même un principe juridique qui confirme l'hypothèse selon laquelle les ordinateurs peuvent apporter un changement qualitatif dans les systèmes d'information, à cause de l'augmentation quantitative de la capacité et du pouvoir de manipulation des données.

"Je me rappelle l'histoire racontée une fois par un professeur de droit pour expliquer la relation qui existe entre ce qui est légal et ce qui risque de devenir illégal. Un fermier possède un cochon, et ceci est tout à fait admissible; il en garde deux, c'est encore admissible; trois, passe encore; mais à partir d'un certain nombre, les cochons peuvent déranger considérablement les voisins. Il en va de même pour les renseignements ou les actes, qui peuvent être parfaitement admissibles par eux-mêmes, mais qui s'ils sont pris ensemble peuvent être considérés par la société comme différents en caractère et en qualité. Je crois, par exemple, qu'il est tout à fait possible qu'en vertu des lois en vigueur dans une certaine administration on puisse interdire aux agences publiques ou privées d'établir des banques de données sur les personnes, même s'il s'agit de données publiques ou de renseignements en grande partie mis à la disposition du public. Je ne recommande pas cette façon de procéder, mais je crois que cela se produira très probablement en ce qui concerne l'établissement par les gouvernements de banques générales de données sur les citoyens."

1. Comment les ordinateurs peuvent empoisonner la vie privée

Le rapport de la conférence contient "l'opinion prédominante" selon laquelle il est vrai que l'ordinateur peut modifier la "qualité" du problème de la violation de la vie privée à cause de son effet sur les systèmes d'information. L'exemple de la R.H. Donnelly, cité par M. VanderNoot, montre l'une des façons dont cela peut se produire, à savoir que par

l'emploi d'un ordinateur pour classer, comparer et intégrer les divers dossiers de données d'une manière vraiment complète, un changement qualitatif peut se produire dans les données elles-mêmes. Il y a cependant plusieurs autres façons dont les ordinateurs peuvent modifier les systèmes d'information, et du même coup violer directement ou indirectement la vie privée des gens.

Il y a lieu de s'arrêter, par exemple, à la prédiction suivante faite par M. Douglas F. Parkhill, du ministère des Communications:

"Les progrès techniques qui ont permis la création des services de téléinformatique¹² ont dangereusement accru le pouvoir qu'ont les gouvernements et certains organismes privés de nous surveiller étroitement. Si on groupait tous les dossiers des différents systèmes: médecine, éducation, finance, affaires, droit, police, on pourrait avoir en main des données complètes et faciles à consulter sur tous les citoyens, de leur naissance à leur mort. Si on permettait à cette situation de se développer sans contrôles adéquats, elle pourrait menacer dangereusement le droit à la vie privée, et si elle était trop poussée, on pourrait aboutir à une société dans laquelle le conformisme deviendrait la clef de la survivance."

Bien que l'ordinateur fasse ici à peu près la même chose que dans le cas de la compagnie Donnelly, il s'agit d'un problème juridique complètement différent. M. Parkhill évoque ici la possibilité que des gouvernements ou des organismes privés intègrent des dossiers de données déjà confidentielles concernant des personnes, peut-être pour des raisons d'efficacité et d'économie, mais qui n'en donnent pas moins une banque de dossiers personnels dont les citoyens n'auraient peut-être jamais approuvé la création si on leur avait demandé leur avis.

Une troisième façon par laquelle les ordinateurs peuvent avoir un effet sur les systèmes d'information est contenue implicitement dans l'image de l'aiguille et de la botte de foin évoquée par M. Deutsch. L'énorme capacité et la vitesse ultra-rapide des ordinateurs permettent aujourd'hui d'établir et d'employer des systèmes d'information auxquels on n'aurait pas pu songer autrefois. C'est pourquoi de nombreux systèmes d'information actuellement en service deviendraient instantanément plus puissants s'ils étaient mis sur ordinateur.

Comme le disait M. A.E. Gotlieb: "Avant la venue de l'ordinateur, les dossiers concernant les diverses activités de chaque personne étaient incomplets et séparés les uns des autres, pour la simple raison que les systèmes classiques ne permettaient pas de traiter efficacement et économiquement de grandes

quantités de renseignements. L'ordinateur, cependant, permet de mettre en mémoire, combiner et transférer des masses de données efficacement et à bon compte."

La quatrième façon dont les ordinateurs peuvent modifier les systèmes d'information, et indirectement violer la vie privée des gens, est leur tendance, qui a été fortement soulignée par M. Hugh Lawford, à transformer les données précédemment "gratuites" en données commerciales. "Parce que les systèmes d'information par ordinateur sont coûteux et peuvent être contrôlés à un point qu'on ne peut atteindre pour les documents privés, je crois qu'il s'exerce des pressions énormes afin de faire de l'information un produit commercial.¹³ Il est donc possible de dire que chaque fois que quelqu'un demande un texte de loi à une banque de données on devrait le faire payer." Par ailleurs, M. Lawford a fait remarquer que lorsqu'il demandait des documents juridiques auprès des gouvernements en vue de les employer dans sa banque de données, il s'est aperçu que les autorités ont commencé à exiger des "compensations financières" pour ce service, ce qu'elles n'auraient pas fait il y a quelques années.

Il est probable que cet élément de coût deviendra s'il est généralisé un autre facteur susceptible d'élargir le fossé qui sépare ceux qui ont le pouvoir (et l'argent) pour se permettre de manipuler l'information et ceux qui se font manipuler.

Finalement, M. Claude-Armand Sheppard, dans son mémoire et dans des déclarations qu'il a faites à la conférence, a parlé d'une cinquième façon par laquelle les ordinateurs peuvent modifier les systèmes d'information et déranger les gens.

"Pour employer des termes directs, c'est la peur qu'ont les gens d'être régis par les ordinateurs. Nous savons bien que c'est une formule par trop simpliste. C'est un fait connu que les ordinateurs conviennent parfaitement pour les tâches répétitives. De fait, on a dit volontiers que les ordinateurs ne pensent pas, ne prennent pas de décisions et n'établissent pas de politiques à suivre. Mais est-ce bien vrai? La plupart des décisions qui doivent être prises par les administrations nécessitent l'application de règles relativement simples à des faits tout aussi simples. Mais pour la personne concernée, ces décisions simples, presque mécaniques, peuvent être d'une très grande importance, car elles déterminent ses droits, sa sécurité et les aspects essentiels de sa vie. Cependant, il est fort probable que ce seront ces décisions qui seront confiées aux ordinateurs.

Jusqu'à présent, les principaux contacts des citoyens avec leur gouvernement ont eu lieu dans des domaines

comme la fiscalité et l'assurance sociale. Ce sont précisément ces domaines que les ordinateurs sont en train de prendre en mains. Ne faites pas l'erreur de sous-estimer l'angoisse que cela déclenchera chez les gens."

Il y a lieu de noter, comme on l'a fait à plusieurs reprises au cours de la conférence, qu'il s'agit là généralement de moyens par lesquels l'ordinateur violera la vie privée si on l'utilise pour les systèmes d'information. Dans ce cas, l'ordinateur viendra soit envahir de nouveaux secteurs, soit s'établir plus profondément dans d'autres. Actuellement, comme l'a fait remarquer M. M.T. Pearson, aucun bureau de crédit du Canada n'utilise d'ordinateur pour la mise en mémoire des renseignements. Seuls les gouvernements ont un nombre important de dossiers individuels sur ordinateur, mais là aussi, on trouve de curieuses lacunes. La Gendarmerie royale, par exemple, n'a pas encore de système à accès direct pour ses dossiers de police.¹⁴ En somme, comme d'habitude, les réalisations concrètes sont un peu en retard sur les possibilités qu'offrent déjà les techniques. Pourtant, on a beaucoup discuté durant la conférence au sujet des possibilités techniques et économiques de l'utilisation des ordinateurs pour la plupart des systèmes d'information.

2. Possibilité financière et technique de systèmes d'information par ordinateurs

Trois animateurs de tables rondes, MM. B.B. Goodfellow, de IBM Canada, D.F. Parkhill, sous-ministre adjoint pour la planification au ministère des Communications et John M. Russell, vice-président de Systems Dimensions Ltd., d'Ottawa, ont parlé des aspects techniques et financiers des systèmes d'information par ordinateur. De plus, il y a eu quelques discussions à ce sujet au cours des ateliers, mais les points importants soulevés lors de ces discussions ont tous été signalés dans les mémoires de ces trois participants.

M. Parkhill a soutenu en général que l'emploi des ordinateurs pour les systèmes d'information est non seulement techniquement et économiquement possible mais qu'il se développe "à un rythme phénoménal." MM. Russell et Goodfellow ont quant à eux souligné les obstacles techniques et économiques qui freinent le développement des systèmes d'information par ordinateur.

"A moins pour le reste de la présente décennie," a dit M. Parkhill, "les développements les plus significatifs dans les systèmes d'information résulteront de la fusion des disciplines auparavant indépendantes des ordinateurs et des communications, qui donnera naissance à ces nouvelles formes d'entreprises que nous appelons "services de téléinformatique."

M. Parkhill a énuméré plusieurs innovations techniques qui rendent cela possible.

1. Il est maintenant possible de mettre à la disposition d'un utilisateur où qu'il soit dans le monde, à condition qu'il dispose des installations de télécommunications appropriées, toute la puissance d'un gros ordinateur.
2. L'interaction entre l'ordinateur et l'utilisateur éloigné est essentiellement instantanée, de sorte que ce dernier reçoit le même service que s'il était sur place.
3. Chaque utilisateur ne paye qu'une petite fraction de la somme qu'il devrait déboursier si le même service était assuré par un ordinateur lui appartenant en propre.
4. Chaque abonné peut accéder rapidement à des dossiers privés, auxquels on peut encore ajouter, et qui sont raisonnablement bien protégés contre l'accès non autorisé.
5. Les réalisations intellectuelles et les données de plusieurs personnes et organismes peuvent être groupées dans des fichiers publics qui pourront être mis à la disposition de tous les utilisateurs du système.
6. La technique du partage du temps a rendu économiquement possible le dialogue direct entre l'homme et l'ordinateur.

M. Parkhill a ensuite décrit quelques systèmes d'information qui seront bientôt mis sur ordinateur, et il a fait voir quelques-uns des effets que les ordinateurs auront sur ces systèmes. Il a averti les délégués qu'une "liste complète des applications possibles ressemblerait à la table des matières de l'Encyclopedia Britannica", mais il a proposé une liste préliminaire de celles qui seraient tout probablement les plus importantes (voir l'Annexe 5).

Parmi les systèmes d'information par ordinateur décrits par M. Parkhill, les plus importants sont peut-être ceux qui sont destinés à des fins pédagogiques.

"A long terme, c'est dans le domaine de l'enseignement que se feront sentir le plus fortement les effets de l'avènement de la téléinformatique. Aussi bien le genre des écoles que le rôle des maîtres vont changer de façon radicale à mesure que le "terminal familial", les

encyclopédies électroniques, les services d'enseignement et d'administration scolaire se développeront. C'est ainsi qu'il faudra peut-être abandonner le principe des classes basées sur l'âge physique des élèves. On les remplacera par un système de paliers répondant aux talents individuels de chaque étudiant. De fait, les services familiaux de téléinformatique permettront aux étudiants de suivre le plupart de leurs cours chez eux. Le temps passé à l'école pourrait être consacré à des travaux de laboratoire, à des discussions de groupe, à des séminaires et à des entretiens particuliers avec les professeurs."

M. John Russell, vice-président (recherche et développement) de Systems Dimensions Limited, d'Ottawa, a présenté lors d'une table ronde quelques-unes des difficultés économiques et techniques qui restreignent l'établissement de grands systèmes d'information par ordinateur à accès direct. M. Russell a soutenu qu'en "utilisant la technologie actuellement disponible, aucune limitation importante de la capacité de mémorisation n'entrave les concepteurs d'un service d'information à accès direct."

"Les mémoires de masse à accès direct actuellement disponibles sur le marché permettent de mettre en mémoire sur ordinateur plus d'un trillion de caractères d'information pour un investissement d'environ 10 millions de dollars. Une telle capacité permettrait d'avoir environ 10,000 mots sur chaque habitant du Canada, au coût d'environ 50 cents par personne."

Selon M. Russell, ces dossiers de données pourraient être mémorisés à bien meilleur compte si on les mettait sur bandes autonomes plutôt que dans des dispositifs à accès direct. "Par exemple, ces dossiers hypothétiques seraient mémorisés sur environ 25,000 bobines d'ordinateur, pour moins de 5 cents par personne."

Un des principaux problèmes techniques des systèmes en direct réside dans la vitesse d'accès à l'information.

"Bien que les temps d'accès et les vitesses de transmission des données puissent être très élevés, quand le concepteur prend en considération les opérations auxiliaires, comme les files d'attente pour l'accès, la recherche de l'emplacement des données, la vérification des mots de passe etc., il serait présomptueux de prédire beaucoup plus qu'environ mille accès par heure. Cela signifie qu'une seule des applications possibles des banques de données, par exemple l'immatriculation des véhicules moteurs, pourrait complètement immobiliser le système

(l'immatriculation de 3 millions de véhicules répartie sur 300 jours, c'est-à-dire 10,000 immatriculations par jour, ou 1,000 à l'heure)."

M. Russell a ajouté que le problème du temps requis pour accéder aux données est plus aigu dans les banques de données employées pour des fins spécifiques que dans celles employées à des fins d'analyse statistique. En d'autres termes, quand on accède à des dossiers de données dans le but de faire des analyses statistiques, on peut les retirer du dispositif de mémorisation, l'un après l'autre, dans l'ordre où ils se présentent. Cependant, dans les cas où on a besoin de données spécifiques, une recherche individuelle (prenant beaucoup de temps) est nécessaire pour chaque rubrique.

M. Russell a également mentionné quelques problèmes de mise en service auxquels tous les exploitants éventuels de banques de données auront à faire face. Par exemple, "le processus de mise sur pied du système nécessitera généralement la transcription des données sous une forme acceptable par l'ordinateur. Peut-être le danger le plus immédiat et le plus menaçant pour un particulier est-il dû à la difficulté d'assurer un contrôle adéquat de la qualité lors de ces opérations de transcription. De plus, il est possible que le dossier d'une personne ne soit pas consulté avant des mois, ou même des années, après la transcription en langage machine, dans ce cas les erreurs peuvent être plus difficiles à corriger." Il a aussi fait remarquer que la transcription "coûte très cher" et que "dans bien des cas le coût peut en être prohibitif".

M. Russell s'est également demandé s'il était mieux d'avoir une banque de données centralisée ou un réseau de banques de données de moindre importance. Mais au sujet de ce réseau, M. Russell a fait remarquer que malheureusement la transmission de données d'un centre à l'autre, par exemple à des fins d'analyse, coûte très cher. A l'appui de cette thèse, voici l'exemple hypothétique qu'il a donné:

"Supposons qu'un chercheur autorisé, dont le bureau se trouve dans un centre régional comme Québec, désire étudier les courbes actuelles de l'état de santé des familles de l'Ontario et du Québec. Ayant en mains un dossier sur ruban, obtenu récemment à la banque de données de la ville de Québec, il demande le dossier correspondant à Toronto. Soulignant le caractère urgent de sa recherche (par exemple, la pollution par le mercure), il demande qu'on lui envoie le dossier de Toronto sur des circuits loués d'une société exploitante de télécommunication.

Or, le dossier ontarien de la santé pourrait comporter six millions de fiches contenant chacune 200 mots

(environ 50,000,000,000 de bits). Du fait qu'à l'heure actuelle les données sont transmises à la vitesse d'environ 50,000 bits par seconde, notre chercheur de Québec devra attendre près de deux semaines pour obtenir l'information dont il a besoin.

Bien que le coût de la transmission ne soit peut-être pas un facteur important dans ce cas, il est intéressant de noter qu'en vertu des tarifs actuels les frais de transmission auraient dépassé les sept mille dollars. On aurait pu avoir recours aux messageries aériennes, qui auraient permis de recevoir les bandes en dix fois moins de temps et à un coût dix fois moindre."

Aux observations de M. Russell, s'ajoutent celles de M. B.B. Goodfellow, de IBM Canada Ltd. M. Goodfellow a parlé principalement des progrès techniques dans la conception des ordinateurs au cours des prochaines années, progrès qui sont appelés à avoir des effets importants sur la viabilité technique et économique des banques de données.

"Aujourd'hui", a-t-il dit, "nous pouvons envisager les technologies qui nous conduiront à des limites absolues dans le perfectionnement des unités de traitement. Vers le milieu des années 1970, on aura probablement des systèmes de 1 à 2 nanosecondes, et au début des années 1980 on devrait parvenir à une amélioration d'un ordre de grandeur de plus avec des circuits de l'ordre de 100 picosecondes. Il semblerait que cette étape atteinte nous en soyons pour quelques temps arrivés à la limite des possibilités d'un ordinateur linéaire."

M. Goodfellow a cependant souligné que "compte tenu de l'expérience très limitée dans la conception des systèmes d'information actuels, on s'attend à ce que le temps de compulsation (de l'unité de traitement à la mémoire centrale) doive être augmenté de 1,000 à 5,000 fois afin que même les systèmes d'information relativement simples soient utiles." Et il ajoutait: "les améliorations prévues des circuits ne permettent pas d'envisager une augmentation de cette importance."

Par ailleurs, en ce qui concerne la mise en place, M. Goodfellow a déclaré: "Il semble à l'heure actuelle que l'on va mettre au point des systèmes polyvalents qui seront contrôlés par un système principal. Un certain nombre d'innovations sont nécessaires dans ce domaine avant que le rendement des systèmes ne réponde aux besoins des banques de données projetées."

Egalement dans le domaine des supports de mémoires de grande capacité, M. Goodfellow a fait remarquer que bien qu'il n'y ait pas de limite à la quantité de renseignements qui peuvent être mémorisés, il est regrettable que plus s'accroît la capacité

de mémorisation plus s'accroît généralement le temps d'accès." M. Goodfellow prévoit des améliorations dans les supports de mémoire au cours de la prochaine décennie, au point où de "très grands systèmes (qui auraient une mémoire à accès direct de l'ordre, par exemple, d'un milliard de caractères ou plus) seront utiles pour l'expansion d'un grand nombre d'applications actuellement en service, mais que leurs temps d'accès seront inacceptables pour l'exploitation en temps réel. Certaines technologies nouvelles pourront peut-être faire sauter certaines des limites auxquelles nous nous butons actuellement, mais ces systèmes semblent impossibles à réaliser pour au moins dix ans."

3. Sécurité des systèmes d'information par ordinateur

Par eux-mêmes, les ordinateurs peuvent modifier les systèmes d'information au point de toucher la vie privée des gens. Cependant, les ordinateurs et les informaticiens ne sont pas toujours à leur meilleur et ne font pas toujours ce qu'ils sont censés faire. Ils font des erreurs et ne réfléchissent pas toujours assez longtemps sur un problème. Les informaticiens, eux, peuvent faire preuve de laisser-aller, de négligence ou simplement de malhonnêteté. Par suite de n'importe lequel de ces avatars, des renseignements compromettants au sujet des gens peuvent être communiqués à des personnes qui ne devraient pas les avoir ou à des gens malhonnêtes. Dans les deux cas, la vie privée des gens pourrait être injustement compromise. Les mesures prises pour éviter de telles éventualités entrent sous la rubrique générale de la sécurité dans l'environnement de l'ordinateur, une question qui a précocoupé un grand nombre de participants à la conférence et qui, on s'en doute, intéresse le public en général.

Comme l'indique un liste de exigences de sécurité fournie par M. Willis Ware, les mesures à prendre sont très différentes de celles qui sont requises pour tout autre milieu. M. Ware énumère cinq exigences.

1. Protection physique du centre d'informatique, et supports de mémoires démontables.
2. Les communications devraient être protégées par un code quelconque ou des appareils de protection des circuits.
3. Tout système à usagers multiples doit avoir des dispositifs capables de protéger le matériel afin d'empêcher un utilisateur de dérégler le programme de contrôle ou les dispositifs de protection du pérogramme.

4. Il faut des dispositifs de protection du périmètre afin de contrôler l'accès aux dossiers, effectuer des vérifications, alerter le personnel en cas de situations anormales, etc.
5. Les contrôles de sécurité doivent aussi prendre adéquatement en considération le personnel de direction et de gestion.¹⁵

En supposant que ces diverses exigences de sécurité soient satisfaites, il reste la question de savoir si les systèmes d'information par ordinateur sont ou seront plus sûrs que les systèmes manuels. Il est évident que cette question est en grande partie hypothétique car on ne dispose actuellement que d'une maigre expérience dans ce domaine. Voici cependant un échantillonnage des opinions et de faits qui ont été présentés lors de la conférence.

M. B.B. Goodfellow, de IBM Canada Ltd., a dit: "Bien que les progrès de la technologie puissent constituer une menace à la vie privée, la même technologie peut jouer un rôle encore plus important dans la protection de la vie privée. Que cela nous plaise ou non, notre vie n'est guère privée de nos jours, et je suis convaincu que les ordinateurs et les banques de données peuvent protéger notre vie privée beaucoup plus que la menacer."

Un exemple concret de cette façon de voir figure dans le mémoire de M. M.T. Pearson concernant le fonctionnement des bureaux de crédit. "Nous sommes d'avis", a-t-il dit, "que l'emploi des ordinateurs donnera lieu en fait à une plus grande précision et à un traitement plus confidentiel des données."

M. Pearson a poursuivi en mentionnant les effets que les ordinateurs auront sur l'exploitation des bureaux de crédit:

"Les ordinateurs permettent aux dossiers de nombreux bureaux de crédit d'être groupés dans une zone commerciale centrale. Pour celui qui accorde le crédit, cela signifie qu'il peut s'adresser à un seul endroit pour obtenir des renseignements au sujet des clients éventuels dans toute la zone qu'il dessert. Pour le client, cela signifie l'ouverture plus rapide de son compte étant donné que le bureau de crédit n'a plus, dans le cas où le client vient de déménager, besoin d'envoyer de demande de renseignements par le courrier dans une autre ville."

"Les ordinateurs peuvent prévenir les erreurs beaucoup plus efficacement que les systèmes manuels. Par exemple, les ordinateurs effectuent beaucoup plus de vérifications sur l'exactitude des données recueillies que ne le font les systèmes manuels. Les ordinateurs

permettent de faire automatiquement la comparaison entre les systèmes automatiques de facturation des crédateurs et les dossiers des bureaux de crédit. Les ordinateurs employés pour la documentation relative à la solvabilité sont tous des systèmes à accès direct. Les corrections d'erreurs peuvent être faites dans ces systèmes aussi rapidement que dans les systèmes manuels. Les ordinateurs permettent de consulter les dossiers très rapidement, et d'annuler les données périmées qui ne devraient plus influencer la solvabilité d'une personne."

"Grâce aux ordinateurs, les bureaux de crédit peuvent faire davantage de vérifications afin de se protéger contre la mauvaise utilisation des dossiers. CREDIPAK, l'ensemble électronique de vérification de la U.S. Associated Credit Bureaux, surveille chaque accès et chaque changement apporté aux dossiers, y compris l'identification du préposé. Aucun poste terminal ne peut accéder aux dossiers tant qu'il n'a pas été activé par un surveillant et tant que l'opératrice du terminal ne s'est pas identifiée elle-même. Les dispositifs terminaux installés dans les bureaux de crédit qui accèdent au poste central ne peuvent pas modifier les dossiers, sauf pour indiquer qu'un dossier a été consulté. Le système fournit aussi une liste de toutes les modifications importantes qui ont été apportées aux dossiers afin que ces derniers soient vérifiés par un surveillant."

Le point de vue de M. Pearson a été appuyé par M. David Booth (I.P. Sharp Associates Ltd., Toronto), qui a décrit en détail le système de sécurité incorporé dans le système à temps partagé de son entreprise. Comme CREDIPAK, le système I.P. Sharp vise à assurer un niveau élevé d'intégrité et de sécurité des dossiers.

Chaque utilisateur possède un numéro de code d'entrée de 7 chiffres. "Bien que ce code puisse rester le même pendant des mois, les utilisateurs peuvent ajouter leur propre mot de passe pouvant avoir jusqu'à huit caractères et le changer à leur gré", a déclaré M. Booth. Une fois que son code a été accepté par l'ordinateur, l'utilisateur peut employer la machine pour effectuer des fonctions mathématiques ou pour mémoriser et exécuter des programmes conçus par lui.

"Le point le plus important à noter est que lorsqu'une fonction est écrite, elle peut être rendue inaltérable afin que personne, pas même le concepteur de la fonction ou l'opérateur de la console ne puisse voir comment le programme fonctionne ou tente de le changer. On ne peut absolument pas modifier la fonction, on ne peut que

l'effacer", a déclaré M. Booth, qui ajoutait: "Non seulement l'utilisateur peut-il protéger son numéro de compte et le contenu de ses programmes, mais il peut protéger les unités de mémoire qu'on appelle "espaces de travail". S'il était nécessaire de mettre en mémoire un programme de sécurité avant qu'il ne soit rendu inaltérable, on pourrait le garder dans un espace de travail, lui-même protégé par un mot de passe ayant jusqu'à 8 lettres.

Le degré de sécurité employé dépend de l'utilisateur. Ce point est important car la sécurité coûte du temps et de l'argent à l'utilisateur."

En dépit des paroles rassurantes de MM. Pearson, Booth et Goodfellow, un malaise considérable s'est manifesté parmi les participants au sujet de la sécurité dans les systèmes d'ordinateur, particulièrement dans ceux qui contiennent ou qui contiendront des renseignements confidentiels concernant les particuliers.

M. J.S. Crowson, du ministère des Communications, a soutenu que "l'ordinateur ne peut pas être meilleur que le système qui le fait fonctionner." Citant l'expérience acquise par le ministère canadien des Postes dans la conception de ses systèmes de mandats postaux, il a ajouté: "On peut concevoir de nombreux systèmes merveilleux qui déjouent les escrocs pendant quelque temps. Pourtant, les voleurs professionnels ont vite fait de trouver le moyen de déjouer le système."

Un autre participant, M. Ware, a mis en doute l'efficacité des méthodes actuelles de sécurité. Il a dit: "Personne ne connaît le genre de dangers dont seront menacées les banques de données. Cela ne facilite pas la tâche de ceux qui doivent concevoir les systèmes de sécurité."

Un autre problème de sécurité découle de la possibilité de sabotage. Cette question a été soulevée par le Professeur Jean Baetz, de l'Université de Montréal. "Je voudrais savoir, dans l'état actuel des choses, jusqu'à quel point sont vulnérables les banques de données sur ordinateur et les systèmes de télécommunications; c'est à dire ce qui arriverait si un grand nombre de gens sur lesquels on cherche à avoir des renseignements décidaient de contrecarrer le système? Par exemple, ils pourraient mentir délibérément, ou donner deux réponses à une question auxquelles on doit n'en donner qu'une."

M. Ware a répondu comme suit "Je peux répondre à cette question, mais ma réponse ne sera pas très utile. Les banques de données sont extrêmement vulnérables. Cette réponse n'est pas très utile car personne ne s'est vraiment penché sur le problème de leur protection dans de tels cas. On peut trouver des moyens

pour se protéger partiellement. Par exemple, supposons qu'une personne ne déclare pas son véritable revenu dans un questionnaire parce qu'elle pense qu'on est trop curieux. Par comparaison avec le revenu d'un nombre suffisant de personnes dont on estime les réponses comme étant correctes, il est possible de rétablir la vérité." M. B.B. Goodfellow a fait remarquer que les systèmes d'information par ordinateur sont "moyennement vulnérables" à l'accès illégal. "Le véritable problème est qu'on ne se sent pas pressé de faire quoi que ce soit à ce sujet. Je suis d'avis que nous saurions quoi faire si le besoin s'en faisait sentir."¹⁶

Chapitre IV

Mesures suggérées

"Divers spécialistes de l'information nous ont parlé d'un monde nouveau, j'hésite à dire le meilleur des mondes, dans lequel les ordinateurs mettront à notre portée toute une gamme de services. Ces spécialistes cependant s'inquiètent au sujet des règlements destinés à protéger la vie privée des gens, car ils craignent qu'on ne réglemente aussi la liberté d'expression. C'est, je crois, ce que le professeur Moifat Hancock appelle une "catégorie transplantée", selon laquelle l'utilisation d'un concept développé pour un contexte complètement différent de celui auquel il est appliqué peut donner à une conclusion ambiguë un certain caractère plausible. Il ne faut pas confondre la liberté d'expression avec les activités de ceux qui manipulent les données. Si on ne réglemente pas le monde nouveau, les manipulateurs de l'information tiendront le haut du pavé, sous le couvert de la liberté d'expression. Il ne faut pas confondre cette activité, qui est une activité de contrôle, avec la liberté d'expression."

-E.F. Ryan
Ontario Law Reform Commission

De nombreuses déclarations et opinions exprimées au cours de la conférence tombaient dans la "catégorie transplantée". Il en a évidemment résulté de l'incompréhension, et même parfois de l'animosité, surtout à cause de l'absence d'un contexte mutuellement compris et accepté. Par conséquent, avant d'examiner en détail les mesures suggérées, il serait bon de passer en revue quelques domaines où l'entente a régné, implicitement ou explicitement, tels qu'on peut les dégager des chapitres précédents. Nous aurons alors un contexte pour énoncer les suggestions.

La vie privée, que l'on n'a explicitement définie ni socialement ni juridiquement, a été finalement considérée comme étant un élément indispensable au sens de la dignité de la personne. La possibilité que doit avoir toute personne de conserver sa dignité est une exigence indispensable de la société démocratique. La vie privée d'une personne, définie peut-être comme le désir d'avoir la paix, repose sur deux principes: être à l'abri des intrusions indésirables lorsqu'on veut être seul, et être à l'abri des manipulations indésirables ou des menaces que pourraient faire ceux qui possèdent les moyens de manipuler les autres. Le besoin de vie privée des gens doit tenir compte des exigences légitimes de la société: le respect des lois, le

maintien de l'ordre, le fonctionnement de l'économie, la modification des règlements, etc.

L'information peut être un instrument extrêmement puissant. Ceux qui le savent et qui en ont légitimement besoin cherchent souvent à se procurer des renseignements au sujet des personnes. C'est cette recherche et l'utilisation qu'on en fait qui peuvent attaquer la vie privée ou la dignité des citoyens. La puissance de l'information, entre autres choses, est relative à la capacité de mémorisation, d'extraction, d'analyse et de corrélation des données. L'emploi d'ordinateurs dans les systèmes d'information et de communications a augmenté énormément cette capacité. Dans la mesure où les nouvelles installations seront disponibles à bon compte, il est à prévoir que de nombreux exploitants de systèmes d'information verront un avantage à y avoir recours. Il faut donc songer également à protéger les citoyens contre l'augmentation des violations de la vie privée lorsque les exploitants de systèmes d'information posséderont ou contrôleront de puissantes installations d'informatique.

Dans ce contexte général, les mesures suggérées peuvent être divisées en deux grandes catégories: celles destinées à protéger directement le droit des citoyens à la vie privée, et celles destinées à restreindre les activités de certains exploitants et utilisateurs de systèmes d'information ainsi que les systèmes eux-mêmes. Ces deux catégories reflètent naturellement deux aspects juridiques du problème posé par les systèmes d'information en ce qui concerne la vie privée: d'une part, accorder un droit aux particuliers, et d'autre part restreindre les activités de certains organismes. En cherchant à protéger la vie privée des citoyens, on a fait des propositions visant soit à limiter les empiètements sur la vie privée, soit à conférer aux citoyens le droit d'accès aux renseignements les concernant qui sont détenus par d'autres. Certains participants ont souligné le besoin de réglementer les systèmes d'information eux-mêmes. D'autres ont signalé qu'il fallait réglementer les activités des exploitants et des utilisateurs des systèmes d'information.

Quelle que soit la méthode adoptée, ceux qui établiront ces garanties devraient avoir présent à la mémoire l'avertissement de M. Willis Ware:

"Du point de vue du particulier, les garanties doivent présenter un caractère de crédibilité. Elles doivent lui paraître réalistes, favorables et compréhensibles. Le libellé des lois destinées au grand public ne devrait pas comprendre d'expressions bizarres comme "mémoires auto-protégées" "mode privilégié" et autres termes inventés par les spécialistes. D'abord, si les lois sont trop spécifiques on peut facilement s'y dérober. C'est comme pour les brevets d'invention, on peut

toujours trouver un moyen de se débrouiller à ce sujet. Mais pis encore, si le grand public ne peut pas les comprendre, les lois ne le rassureront pas. On en sera encore revenu au même point."

Les règlements ne devraient pas seulement être compréhensibles et vraisemblables, ils devraient également prévoir les changements inévitables qui sont amenés par les progrès techniques. M. Thomas McPhail, appuyé par M. VanderNoot, a demandé qu'on prenne en considération le rôle grandissant de la recherche en sciences sociales.

M. McPhail a déclaré: "Ceux qui proposent des lois qui limiteraient sévèrement les droits des chercheurs devraient considérer toutes les implications possibles des lois. A une époque où les changements accélérés, les nouveaux modes de vie et le développements de comportements "non-conformistes" sont la règle, les statistiques sociales deviennent presque obligatoires, si les gouvernements et les institutions privées veulent être en mesure d'évaluer les programmes actuels et, ce qui est plus important, de définir les tendances futures de la société et des programmes."

1. Droit à la vie privée

Pour protéger la vie privée, il faut tout d'abord commencer par définir ce que l'on veut protéger. Les tentatives de définition commencent généralement par l'Article 12 de la Déclaration universelle des droits de l'homme des Nations Unies.

"Personne ne sera assujetti à des interférences arbitraires dans sa vie privée, sa famille, son foyer ou ses correspondants, ou à des attaques ternissant son honneur et sa réputation. Tout le monde a le droit d'être protégé par la loi contre de telles interférences ou attaques."

Par elle-même, cette déclaration ne facilite guère la définition de la vie privée. On a dit également que le droit à la vie privée est le droit "d'avoir la paix". Ce concept semble couvrir les principaux dangers que les systèmes d'information font courir à la vie privée, à savoir, les enquêtes sur les activités des gens et la menace posée par ceux qui utiliseraient les systèmes d'information pour manipuler les gens. Rappelons le concept de M. Allan Gotlieb, qui associe le droit à la vie privée au droit qu'a une personne de se débrancher.

"Dans le domaine de la vie privée, on peut trouver le désir d'avoir la paix, de vivre sans être ennuyé par le reste des gens. Cela signifie qu'il faut suffisamment d'espace pour ne pas être gêné par ses voisins, pour mourir seul si on le veut, vivre en dehors de la

société, être non productif, être différent, être un étranger, se débrancher si on le désire. Cela peut également comprendre le respect de l'anonymat dans un lieu public. La vie privée peut également signifier que l'on peut établir des relations intimes avec d'autres personnes en étant assuré que ce qui se passe entre les personnes en cause ne sera pas rendu public."

M. Gotlieb a par ailleurs soutenu que le droit de savoir, ou la liberté d'information, est une exigence vitale dont on doit tenir compte avant d'établir le droit à la vie privée.

"Dans quelle mesure est-il possible de protéger la vie privée des personnes dans une société qui se constitue de plus en plus elle-même comme un énorme système d'information?" Ensuite, M. Gotlieb a parlé d'une situation menaçante dans laquelle un nombre de plus en plus réduit de personnes très compétentes possèdent et manipulent l'information.

"Cela accroît le danger que s'élargisse le fossé qui existe entre les administrateurs et le reste de la société. Les citoyens peuvent en venir à se sentir de plus en plus épiés dans une société dominée par des systèmes d'information."

M. Turner, ministre de la Justice, semblait d'accord et a dit: "Le droit à la vie privée et le droit d'être informé ne sont pas contradictoires mais complémentaires. Le droit à la vie privée et le droit à l'information sont les deux libertés jumelles qui sont nées de la société démocratique et qui lui sont indispensables."

Quelle que soit la façon dont ces droits sont définis, le véritable problème est de les interpréter et de les appliquer dans des cas bien spécifiques. M. Willis Ware, par exemple, semblait vouloir se contenter qu'une revendication contestée en matière de vie privée soit tranchée par les tribunaux.

"Supposons que je m'oppose à l'utilisation que l'on veut faire de certains renseignements à mon sujet qui se trouvent dans une certaine banque de données. J'intente une poursuite. Si je gagne mon procès, il existera un précédent fort utile pour les plus grand bien des particuliers, et tous les exploitants de banques de données en prendront bonne note. Si je perds mon procès, je dois en tant que citoyen conclure que cette catégorie de renseignements a été jugée par la société et par les tribunaux comme étant nécessaire au bien-être de l'ensemble de la société. Dans ce cas, je devrais me soumettre."

Malheureusement, cette façon de voir est probablement trop simpliste. Les participants ont posé beaucoup de questions sur la façon dont un tel droit pourrait être exercé. Devrait-il, par exemple, y avoir un "crime" ou un "préjudice" contre la vie privée, pour lequel seraient prévues des réparations ou des dédommagements? Qui pourrait jouir du droit à la vie privée? Un atelier s'est demandé comment formuler un droit de vie privée pour les particuliers sans qu'en bénéficient également les entreprises et les gouvernements. Par ailleurs, de nombreux délégués ont reconnu que les invasions de la vie privée sont plus susceptibles de causer des dommages psychologiques que des dommages physiques, et que la compensation pour les dommages psychologiques est, pour le moins, une procédure juridique nébuleuse.

M. H.A. Leal, de l'Ontario Law Reform Commission, a cependant insisté sur l'importance d'accorder une compensation aux personnes qui ont été lésées dans leur dignité. "Je me rends compte que M. Westin est d'avis que les mesures de dédommagement sont trop brutales dans le cas de personnes qui ont été lésées par une erreur causée par une personne, une machine, ou autrement. Je crois pourtant qu'en plus des procédures réglementaires, des normes et des sanctions pénales, ces mesures sont les seules qui permettent de pénétrer dans le vif de l'injure." Ce point de vue a été appuyé, entre autres, par M. Parkhill, qui a réclamé le droit d'être dédommagé en cas d'invasion de la vie privée.

L'explication la plus cohérente peut-être des difficultés rencontrées dans l'établissement d'un droit à la vie privée est celle qui figure dans un rapport sur la protection de la vie privée, rédigé en 1968 pour l'Ontario Law Reform Commission. Les auteurs de ce rapport ont proposé que soit reconnu un crime et un préjudice en matière de vie privée, mais ils ont également soutenu qu'en dépit de son utilité ce geste ne fournirait pas aux particuliers une protection adéquate.

"La protection de la vie privée pose de graves problèmes de nature sociale, psychologique, économique et morale qui ne se prêtent absolument pas aux tentatives de solution basées sur des catégories juridiques existantes, ou à tout ce qui n'est pas une législation qui envisage toutes les possibilités. Si l'objectif est d'assurer une protection de la vie privée qui soit raisonnable pour tous les cas qui se présentent, la loi ne doit pas seulement définir les revendications relatives à la vie privée comme telle, mais elle doit également définir les revendications contraires qui sont basées sur des considérations comme l'intérêt public, le bien-être économique, l'efficacité commerciale et le contrôle des activités antisociales. Si on omettait de créer des normes parallèles, particulièrement dans les domaines où règne soit une forte tradition de laissez-

faire, soit un ensemble bien établi de valeurs institutionnelles propres, alors les exceptions inhérentes pour protéger la vie privée d'une façon qui soit "raisonnable dans toutes les circonstances" pourraient bien l'emporter sur la règle. La perte de la vie privée, et la diminution de la qualité de la vie qui en découle, est en réalité le sous-produit de centaines de tentatives bien intentionnées visant à résoudre les grands problèmes de notre société urbaine et industrielle par l'utilisation des progrès techniques et de pratiques commerciales simplifiées, et à y parvenir avec le moins de temps, de ressources et d'efforts possibles. Les moyens de contrôle envisagés par suite de la crainte que l'ensemble de ces tentatives ne soit pas raisonnable, mais dont l'efficacité ne dépend que d'une question, à savoir si une partie quelconque de l'ensemble n'est pas raisonnable, semblent voués à l'échec. Si nous nous préoccupons de la dégradation de la qualité de la vie, alors l'ampleur de nos actions futures doit correspondre à l'ampleur de ce qui nous préoccupe. La création de restrictions générales des moyens et des intérêts qui menacent cette qualité de la vie constitue en fait l'essentiel de la protection de la vie privée. La simple définition d'un droit à la vie privée, sans rien de plus, n'en est qu'une pâle image."

Bien que l'Ontario Law Reform Commission soutienne ici que la reconnaissance d'un droit à la vie privée pourrait ne pas faire beaucoup de bien, de nombreux délégués ont déclaré qu'elle pourrait faire beaucoup de mal, particulièrement si ce droit devait limiter la liberté d'expression et le droit de savoir. M. Hugh Lawford, de l'Université Queen's, a dit par exemple: "Aucune loi ne devrait être adoptée pour protéger la vie privée sans être accompagnée d'une loi visant à protéger la liberté de l'information." La plupart des délégués ont paru approuver cette déclaration comme on peut le voir dans cet extrait du rapport de la conférence:

"Les membres de dix ateliers ont été presque complètement d'accord sur la nécessité de la liberté d'accès à l'information. Cette nécessité a été considérée comme très importante pour ce qui est des gouvernements. Et de nombreux délégués ont reconnu qu'une loi relative à la liberté d'accès à l'information, semblable à celle en vigueur aux Etats-Unis, était nécessaire au Canada."

Bien que la question n'ait pas été spécifiquement posée lors de la conférence, il vaut la peine de se demander si le droit à l'information est implicite dans le droit à la vie privée. En d'autres termes, en supposant qu'une partie du droit à la vie privée soit le droit de "libérer" des renseignements

personnels compromettants qui sont détenus par d'autres, alors peut-être un particulier pourrait-il revendiquer des dommages auprès d'une entreprise qui chercherait à conserver ces renseignements pour le faire chanter. M. Allan Gotlieb, comme on l'a indiqué ci-dessus, considère certainement que le fait d'être à l'abri de toute manipulation est une exigence préliminaire essentielle de la vie privée. Cependant, M. Gotlieb pense que "la loi est incapable d'empêcher que s'élargisse l'écart entre les personnes qui manipulent l'information et les personnes au sujet desquelles l'information est manipulée."

Que le droit à l'information soit considéré comme une partie intégrante du droit à la vie privée ou comme un droit par lui-même, la même série de questions posées ci-dessus par l'Ontario Law Reform Commission à l'égard de la vie privée peut s'appliquer au droit à l'information. Est-ce que la reconnaissance d'un droit à la vie privée ou d'un droit à l'information permettrait de protéger adéquatement les gens contre les dommages faits par d'autres qui exercent des droits légitimes mais opposés? En tout cas, il est probable que le Canada établira des lois distinctes afin de protéger le droit à l'information. Le professeur Lawford et M. Turner, ministre de la Justice, ont tous deux cité d'autres raisons qui n'étaient pas directement liées à la question de la vie privée pour justifier l'adoption de lois qui garantiraient aux citoyens le droit à l'information. On se souviendra que l'une des principales raisons est la nécessité pour les citoyens d'accéder aux documents gouvernementaux afin de pouvoir participer activement au régime démocratique. Le ministre de la Justice s'est montré très favorable à l'adoption d'une loi sur la liberté d'accès à l'information.

"Il nous faut une loi sur la liberté d'information, qui permettrait aux citoyens d'obtenir des données que les autorités gouvernementales ont arbitrairement décidé de ne pas rendre publiques. Il est vrai, comme l'a fait remarquer le professeur Lawford, que le gouvernement canadien n'a pas encore adopté une loi concernant l'accès aux documents officiels. En ce qui concerne l'accès aux documents classés dans les archives nationales conformément à la Loi sur les archives, et en ce qui concerne les documents qui sont encore conservés dans les ministères, la situation est loin d'être satisfaisante. Il est vrai que certains types de renseignements gouvernementaux ne doivent pas être rendus publics. Cependant, les critères ainsi que la non diffusion de ces documents devraient être clairement énoncés dans les statuts. Le public aurait ainsi des renseignements sur ce qui constitue un document gouvernemental confidentiel, et il pourrait au moins être au courant des raisons pour lesquelles le gouvernement doit garder le secret. Par exemple, le

Freedom of Information Act, adopté par le Congrès américain en 1966, et qui avait pour but de rendre les dossiers administratifs plus accessibles au public, énumère huit catégories de données compromettantes qui doivent rester secrètes. Ces catégories comprennent, entre autres, les documents se rapportant à la défense nationale ou à la politique étrangère dont le secret a été autorisé par ordre du Président.

L'exception la plus intéressante est peut-être celle qui concerne les questions comme l'emploi, les services médicaux, etc., dont la révélation constituerait une invasion clairement non justifiée dans la vie privée. En fait, la caractéristique importante du Freedom of Information Act, qui n'est pas d'ailleurs assez connue, est que la loi vise autant le droit à la vie privée que le droit à l'information. L'un des objectifs de cette loi était de fournir un critère sur lequel se baser pour empêcher la diffusion de données recueillies par le gouvernement au sujet des citoyens. Les deux droits ne sont donc pas contradictoires mais complémentaires; ce sont deux libertés parallèles et non opposées, qui sont nées de la société démocratique et qui lui sont indispensables."

Si on accepte la thèse formulée par l'Ontario Law Reform Commission, et par un grand nombre d'autres, le geste relativement simple qui consiste à reconnaître le droit des personnes à la vie privée et le droit à la liberté d'information ne suffira pas pour protéger les citoyens contre les invasions de la vie privée dans la société urbaine et industrielle actuelle. De plus, il semble nécessaire d'adopter des lois pour restreindre les activités de nombreux organismes, personnes ou dispositifs qui pourraient, intentionnellement ou accidentellement, violer la vie privée des gens. La liste de ces envahisseurs éventuels devrait comprendre l'utilisation de tables d'écoute, de dispositifs de surveillance, etc. Le mandat de la conférence tenue à l'Université Queen's se limitait cependant au domaine des ordinateurs, des systèmes d'information et des activités des exploitants et des usagers de ces systèmes. Mais on a cependant reconnu que des mesures devaient aussi être prises à leur sujet. M. J.M. Sharp, professeur de droit à l'Université du Manitoba, a déclaré ce qui suit à ce sujet: "l'entrée, la mémorisation et la sortie des données ne doivent pas être réglementées par la bonne foi des exploitants eux-mêmes. Même avec la meilleure volonté du monde, les exploitants des banques de données ne peuvent pas garantir que la vie privée des gens sera protégée, à moins que des sanctions légales ne soient là pour donner du poids à leurs bonnes intentions."¹⁷

2. Comment empêcher les abus dans l'utilisation des systèmes d'information

"Ce qui m'inquiète, c'est qu'en cherchant à réglementer les problèmes actuels on soit amené à développer des règles si générales qu'elles risquent de gêner les systèmes de l'avenir, qui ne sont pas menacés par les mêmes dangers."

-Hugh Lawford

"En fixant les règles de la circulation avant que la route ne soit utilisée, on peut éviter de graves collisions."

-A. E. Gotlieb

Comme dans toutes les discussions relatives à une législation destinée à restreindre les activités de certaines personnes et de certains organismes, il y a eu des éperviers et des colombes. La couleur du plumage semblait dépendre de la mesure dans laquelle chacun craignait que les mesures juridiques gênent les progrès technologiques. Le dilemme a suscité une atmosphère très tendue. Derrière les positions apparemment calmes et raisonnées de ceux qui préconisaient pour dès maintenant l'établissement d'une législation générale et ceux qui avertissaient de ne pas toucher à la technologie, se dessinaient des menaces voilées de chaos. Et le juste milieu du bon sens, si il en existe vraiment un, ressemblait beaucoup plus à un sentier tortueux et semé d'embûches qu'à une route droite et dégagée.

M. B.B. Goodfellow, de IBM Canada Ltd., s'est dit inquiet au sujet de la "législation excessive d'un aspect limité d'un problème d'envergure. Les normes étouffent l'innovation." Ce point de vue a été appuyé par au moins un atelier, qui a déclaré ce qui suit: "Il serait très dangereux d'essayer d'être trop général pour commencer. Cela risquerait de restreindre ou de retarder les progrès de la technologie."

Parlant au nom des "éperviers", M. Willis Ware a déclaré: "Je ne voudrais pas voir les banques de données devenir un problème du genre de celui de la pollution. C'est pourquoi je suis d'avis qu'il faut formuler avec vigueur les garanties, les lois et les mécanismes appropriés. Essayons de contrôler la situation avant qu'il ne soit trop tard."

De nouveau, le problème du contexte (ou son absence) est probablement en grande partie responsable de cette apparente polarisation de l'opinion. Il est possible de formuler des lois ou des règlements qui pourront adéquatement protéger le public sans restreindre les innovations technologiques. Il sera en fait probablement plus difficile de convaincre les gens de la possibilité de le faire que de le faire vraiment.

Prenons par exemple le plus simple des deux aspects du défi que posent les systèmes d'information, à savoir qu'il faut veiller à ce que le personnel soit compétent, honnête, etc. On pourrait s'attendre à trouver une grande différence d'opinion entre les exploitants de systèmes d'information et les planificateurs en ce qui concerne l'intervention du gouvernement dans ce domaine. En fait, personne n'a nié la nécessité de cette intervention. Il y a eu quelques discussions quant à la meilleure façon d'assurer un personnel qualifié, mais il n'y en a pas eu sur le principe. Voici ce qu'a dit M. Willis Ware à ce sujet: "Je veux être protégé contre la possibilité que l'exploitant ne soit pas aussi honnête que je ne le pense. Je veux des garanties légales."

Au cours du débat, M. Mers Kutt, ancien président de la Canadian Information Processing Society, et M. Thomas McPhail, de l'Université Loyola, ont prôné l'auto-réglementation des groupes professionnels.

Parlant au nom des informaticiens, M. Kutt a dit: "La première responsabilité des associations d'informaticiens est de renseigner leurs membres afin qu'ils soient conscients du problème et des droits des personnes, afin qu'entre autres chose ils n'utilisent pas par inadvertance les dossiers. La deuxième responsabilité de ces associations est l'établissement de normes professionnelles et d'un code d'éthique pour tous ceux qui oeuvrent dans le domaine de l'informatique".

Parlant en faveur des spécialistes en sciences sociales, M. Thomas McPhail a fait la suggestion suivante: "Il se peut que la solution la plus fondamentale ne se trouve pas dans la législation mais plutôt dans l'établissement de normes professionnelles élevées pour l'admission de tous ceux qui désirent faire de la recherche en sciences sociales. Un résultat pratique de cette solution serait l'adoption par les sociétés savantes du Canada d'un certain code ou d'une déclaration d'éthique scientifique." Cependant, M. McPhail a également préconisé des mesures gouvernementales qui renforceraient le code d'éthique professionnelle. "En Amérique du Nord", a dit M. McPhail, "il y a approximativement 40,000 spécialistes en sciences sociales. Il suffirait que quelques-uns d'entre eux ne respectent pas leur code d'éthique pour que soit ternie la réputation de cette profession."

Ceux qui ont préconisé une intervention gouvernementale n'ont pas été d'accord sur la forme que cette intervention devrait prendre. M. D.F. Parkhill, du ministère des Communications, et M. J.M. Sharp, de l'Université du Manitoba, ont soutenu que tous les employés des entreprises de systèmes d'information devraient posséder un permis spécial et être cautionnés. Cette suggestion a semblé être appuyée par la plupart des participants à la conférence, et elle n'a pas donné

lieu à de grandes discussions. Une autre suggestion intéressante a cependant été faite par M. John Russell, de Systems Dimensions Ltd., d'Ottawa.

"Les législateurs et les informaticiens reconnaissent qu'il faut rassurer les citoyens quant à l'intégrité du personnel technique qui a la possibilité d'accéder à leurs dossiers personnels. C'est dans ce but que l'on a proposé la formation d'une association professionnelle groupant ceux qui travaillent dans l'informatique, et à laquelle le gouvernement délèguerait la tâche de réglementer, comme c'est le cas pour les associations professionnelles de médecins, d'avocats, de comptables agréés, etc.

Une telle association pourrait assumer deux grandes responsabilités. La première serait d'établir des normes professionnelles suffisantes pour que le public sache que les ingénieurs qui conçoivent les banques de données ont la compétence voulue pour y insérer des dispositifs adéquats de contrôle et de sécurité. La deuxième responsabilité d'une telle association serait de surveiller le recrutement du personnel afin de garantir la sécurité.

Il faudrait de nombreuses années pour qu'une association de ce genre atteigne un haut degré d'efficacité. Dans un milieu qui exige une adaptation rapide et continue à de nouvelles technologies, on peut se demander si une telle association serait jamais en mesure de se tenir au pas de la compétence de ses membres.

Dans l'esprit du public, le problème touchant la sécurité plutôt que le professionnalisme, je pense que son intérêt serait mieux servi si on avait tout simplement recours à des vérifications pour ce qui est du personnel. L'application pure et simple des critères d'emploi utilisés pour les postes confidentiels du gouvernement et de l'industrie devrait être suffisante pour assurer la protection de la vie privée des gens."

De nombreuses propositions, difficiles à concilier, ont été faites en ce qui a trait aux moyens de contrôler les systèmes d'information eux-mêmes. Le professeur J.M. Sharp, par exemple, a suggéré que "chaque banque de données devrait avoir une licence, quel qu'en soit l'exploitant: organisme du gouvernement, compagnie d'assurance, bureau de crédit, compagnie de prêt, etc." D'autres délégués ont même suggéré que certaines catégories de banques de données soient déclarées illégales. Un des participants, lui-même employé dans une banque de données et visiblement ennuyé par la discussion, a quand même vu un bon côté à la chose. M. Ian Sharp, président de I.P. Sharp Associates

Ltd., de Toronto, s'est levé à la fin de la dernière séance plénière pour faire le commentaire suivant:

"Avec la possibilité que le Livre blanc de M. Benson devienne une loi, on pourrait établir une banque de données contenant un si grand nombre de renseignements sur les biens de tous les citoyens du Canada que je voudrais suggérer que toute loi soit libellée de façon à rendre illégale la mise sur pied d'une telle banque de données."

On n'a jamais réglé la question de savoir quelles banques de données pourraient exister et lesquelles d'entre elles devraient être réglementées. Un atelier a fait savoir qu'un "certain accord" avait été obtenu sur le fait que seules les banques de données "qui risquent de faire du tort aux gens" devraient être réglementées. Dans le rapport de la conférence on peut lire que "toutes les banques de données sur les personnes devraient avoir une licence, mais les conditions requises pour la délivrance de cette licence pourraient varier selon la catégorie des renseignements qui y sont mémorisés."

Ayant établi, par un moyen comme le système de classification du professeur C.C. Gotlieb, quels sont les systèmes d'information qui nécessitent un contrôle dans l'intérêt du public, le problème qui se pose encore est celui de la mise au point d'un système adéquat de surveillance. Le Dr Willis Ware a présenté la liste complète des renseignements qu'il aimerait avoir au sujet des banques de données, s'il devait être chargé de les réglementer.

"Avant de délivrer une licence au propriétaire ou à l'exploitant d'une banque de données, je demanderais qu'il fournisse à un organisme de réglementation des indications comme celles énoncées ci-dessous:

*nature et but de la banque de données; à quoi serviront les renseignements recueillis; genre de clientèle qui sera desservie;

*identification et description précises des sources d'où proviendront les données et des vérifications qui seront faites pour s'assurer de l'exactitude des renseignements;

*description complète des garanties du système (moyens physiques, techniques, périgrammes, communications, personnel, direction) destinées à protéger les données et à contrôler leur diffusion;

*description complète des garanties de procédure (périgramme ou employés) destinées à déceler les

erreurs, à classer les données dans les dossiers appropriés, à résoudre les ambiguïtés dans l'identification des personnes, à traiter les renseignements dont l'exactitude est douteuse et à établir les niveaux de confiance applicables à des renseignements qui sont déduits à partir de données fragmentaires;

*description complète des dispositifs de vérification incorporés dans le système, et les résultats de cette vérification qui seront disponibles pour les révisions périodiques;

*mécanisme grâce auquel les particuliers pourront consulter leurs dossiers (qui établira les sources ayant servi à le constituer), mettre en doute leur contenu et corriger les erreurs;

*inspections et essais ayant été effectués sur le système pour s'assurer qu'il fonctionne comme il faut, et tout particulièrement que le pérogramme a été vérifié après qu'il a été complètement assemblé."

M. Ware a également expliqué pourquoi les exploitants de banques de données devraient être obligés de respecter ces exigences qui, à son avis, sont très strictes. "J'aimerais mieux commencer avec fermeté", a-t-il dit, "pour ensuite lâcher un peu la bride, si l'expérience le justifie, plutôt que d'avoir à resserrer la bride après coup." Certaines des exigences qu'il a suggérées, comme la vérification des sources et les mesures de sécurité qui devront être prises pour protéger les banques de données, sont évidemment très importantes. Même si cela n'est pas aussi évident, il reste que ses autres exigences peuvent être tout aussi importantes.

Considérons, par exemple, certains des problèmes qui pourraient se poser au sujet des utilisateurs. M. Ware a soutenu que les exploitants doivent assumer la principale responsabilité en ce qui a trait à l'identification des utilisateurs. Ils doivent, en particulier, tenir à l'écart les indésirables. Ainsi, "les dispositions relatives au caractère secret des communications semblent applicables, étant donné que les utilisateurs recevront des renseignements sous forme de communiqué privilégié et devront être tenus responsables s'ils communiquent des renseignements à des tiers, volontairement ou accidentellement."

Si l'un des utilisateurs était une autre banque de données, M. Ware exigerait de l'exploitant des garanties supplémentaires. "L'exploitant devrait avoir une méthode de vérification qui lui permette de savoir où se trouvent les copies des différentes données dans les dossiers de l'ordinateur. Par

ailleurs, l'exploitant doit accepter la responsabilité de mettre à jour ou de corriger rapidement ces copies. S'il reçoit des données en provenance d'une autre banque de données, il doit conserver suffisamment d'indications afin que les sources originales puissent être identifiées plus tard. Ces indications pourraient être extrêmement importantes dans le cas d'un procès pour dommages dans lequel la responsabilité de l'exploitant serait partagée avec les sources de données." M. Ware croit que les lois actuelles telles qu'appliquées par les tribunaux peuvent être utilisées efficacement afin d'établir les détails précis du droit à la vie privée d'une personne.

Lorsque les autorités chargées de la réglementation auront établi le genre d'information qu'il leur faut pour remplir leurs fonctions, elles devront fixer plusieurs séries d'exigences minimales pour les diverses catégories d'opérations des banques de données, et prévoir des sanctions pour le cas où ces exigences ne seraient pas respectées. A en juger par les discussions qui ont eu lieu lors de la conférence, les délégués étaient très inquiets au sujet des opérations de mémorisation, de vérification et de divulgation des renseignements de certaines banques de données. Par exemple, le professeur J.M. Sharp a passé en revue quelques-uns des dangers qui pourraient résulter de la liaison entre deux banques de données, et il a demandé "qu'on examine de près" cette pratique.

"Ce genre d'enquête aurait l'importance la plus grande dans le cas des banques de données qui ont des liaisons internationales. On a dit, et je suis de cet avis, que l'exportation dans d'autres pays de données personnelles, commerciales et même gouvernementales, pourrait sérieusement menacer l'économie canadienne et violer la souveraineté du Canada de façon bien réelle, même s'il s'agit d'une violation intangible et "invisible".

La réglementation des liaisons entre des banques situées dans des provinces différentes est à peine moins cruciale. Il est certain en effet que l'intégration dans une seule banque de données de renseignements provenant de nombreuses sources est beaucoup plus importante que chacune de ces sources prises séparément.

A l'intérieur des provinces aussi, et particulièrement dans les plus grandes et les plus "industrialisées", le même problème se pose. Les systèmes fonctionnant à l'intérieur des provinces, même s'ils ne sont pas reliés à l'extérieur, devraient être soumis à des règlements provinciaux. Encore ici, il semble nécessaire d'avoir les mêmes règlements dans toutes les provinces.

Il y a lieu de considérer le sujet connexe de la vente de renseignements par les exploitants de banques de données. On a récemment lu dans les journaux qu'une entreprise américaine de données qui avait fait faillite avait vendu au plus offrant, à titre d'actif réalisable, des dossiers concernant 3 millions de personnes. Il est scandaleux de voir des renseignements qui ont peut-être été fournis par des particuliers dans un but très précis, et qui sont probablement confidentiels, ainsi étalés sur la place publique et vendus comme de vulgaires marchandises en réclame.

Il est fortement recommandé que les liaisons réciproques entre les banques de données et les renseignements qui en proviennent fassent l'objet d'une réglementation précise, même au point de faire entrer dans les lois un nouveau concept de "droit du dépositaire", aussi bien en ce qui concerne les bandes, les cartes et autres éléments matériels de l'ordinateur, qu'en ce qui concerne l'information intangible qui provient de ces éléments. Les précédents juridiques qui existent dans ce domaine ne sont pas à même à l'heure actuelle de couvrir toutes les situations, et il est peu probable que la jurisprudence ultérieure puisse le faire assez rapidement et assez complètement."

M. Claude-Armand Sheppard a soutenu dans son mémoire que "les données fournies par les citoyens à un ministère ou à un organisme officiel, à n'importe quel niveau, ne devraient pas être mises à la disposition d'un autre ministère ou de tout autre organisme ou personne à quelque niveau que ce soit." M. Sheppard a par ailleurs affirmé qu'il s'opposait à ce que le gouvernement ou l'entreprise privée établissent de grands centres de données, et qu'il était "opposé à ce que les banques de données gardent en dossier toute référence ou indication concernant les origines ethniques, les croyances religieuses et les opinions politiques des particuliers, sauf à des fins purement statistiques."

M. Parkhill a réclamé "qu'on reconnaisse que la personne dont le dossier contient le nom soit le propriétaire ultime de ce dossier et que, par conséquent, elle seule puisse avoir le droit de décider qui d'autre y aura accès." Allant plus loin, M. Parkhill a suggéré que ceux qui accéderaient au dossier d'une personne sans y être pleinement autorisés devraient être passibles de sanctions sévères en vertu du Code criminel.

En ce qui concerne la réunion et la vérification des données, des propositions ont été faites pour élaborer des mécanismes qui permettraient aux gens de vérifier les renseignements à leur sujet qui sont gardés dans les banques de données, d'empêcher la mémorisation de renseignements qui

auraient été obtenus de la part des voisins et d'établir à l'avance des dates d'annulation pour certains types de renseignements.

M. Parkhill a suggéré que "les exploitants des banques de données aient la responsabilité d'envoyer aux personnes nommées dans leurs dossiers un relevé mensuel des renseignements qui les concernent, le nom des personnes et des organismes qui ont consulté ces dossiers, quel en était le but et qui les en avaient autorisés." Le projet de loi sur les banques de données que M. Tim Reid a déposé à la législature ontarienne contient une disposition à cet effet.

M. Parkhill a également suggéré "que toutes les personnes concernées puissent consulter leur dossier n'importe quand, afin d'en vérifier le contenu et, en cas de désaccord, exiger la suppression des données litigieuses jusqu'au moment où l'exploitant de la banque de données pourra prouver devant un tribunal indépendant que ces données sont conformes à la vérité."

Ce droit à la vérification des données par les personnes concernées a été mentionné dans plusieurs rapports d'atelier; il s'agit donc d'une préoccupation sérieuse et générale.

Le professeur Sharp a cependant concédé certaines réserves au droit réclamé. "Cette vérification pourrait être coûteuse; il faudrait faire payer une somme appropriée aux personnes qui vérifient leur dossier. Cela dédommagerait l'exploitant et empêcherait qu'on le fasse seulement pour le plaisir de la chose."

M. Pearson, de l'Associated Credit Bureaus of Canada, s'est vigoureusement opposé à ce que les exploitants envoient des relevés mensuels aux personnes concernées pour leur faire connaître l'usage que l'on fait de leur dossier. Il a signalé que le gouvernement des Etats-Unis avait rejeté une proposition semblable à cause des frais prohibitifs qu'entraînerait sa mise en application. Un atelier a noté que "l'envoi d'un relevé ne devrait pas être nécessaire si les personnes concernées peuvent avoir accès à leur dossier et qu'elles savent où est gardé ce dossier." Un autre atelier, par contre, a signalé que "l'accès pourrait donner lieu à des injustices par suite de la situation financière des personnes concernées." M. Pearson a également prétendu que la plupart des gens ne désirent pas voir leur dossier de solvabilité car ils se savent solvables, et qu'ils ne tiennent pas à ce que les données qui les concernent soient expédiées par la poste.

Selon un délégué, le haut degré de précision des renseignements détenus par les organismes privés comme les bureaux de crédit résulte de la concurrence. La vérification de la précision se fait naturellement lorsque l'entreprise qui vend

des renseignements doit faire face à la concurrence. Par contre, une plus grande attention est selon lui nécessaire dans les cas où il n'y a pas de concurrence.

Le professeur Sharp a déclaré que certains renseignements devraient être enlevés des dossiers une fois écoulée une période de temps déterminée d'avance. Il a fait remarquer que l'Associated Credit Bureaus Inc., de Houston au Texas, a pour politique de ne pas rapporter les faillites vieilles de plus de 14 ans à partir de la date d'adjudication de la plus récente faillite, et de ne pas garder en note pendant plus de sept ans les données relatives aux comptes mis en perception. "Bien que l'on puisse soutenir", a dit M. Sharp, "que les dates d'annulation ne devraient pas s'appliquer à certaines banques de données gouvernementales (comme par exemple celles du Bureau fédéral de la statistique, qui dépersonnaliserait les données avant de les rendre publiques), on accepte généralement, pour protéger la vie privée des gens sans pour autant faire tort à la liberté d'accès à l'information, que des dates d'annulation devraient s'appliquer à certains renseignements une fois écoulée une période de temps donnée."

Pour accélérer les choses, M. Ware a suggéré que "la personne devrait probablement avoir un document juridique qui attesterait que certaines dispositions ont été prises. Considérez le cas d'une personne ayant été arrêtée et accusée d'un crime. Elle est cependant acquittée par la suite. Son arrestation pourrait fort bien avoir été signalée dans son dossier de solvabilité; la banque de données devrait donc lui fournir une attestation à l'effet que la référence à son arrestation a été supprimée dans toutes les copies de son dossier."¹⁸

Finalement, MM. B.B. Goodfellow et John M. Russell ont donné quelques conseils techniques aux législateurs et aux personnes qui promulgueront les règlements. Voici un extrait de la déclaration de M. Goodfellow:

"Les systèmes d'information de la défense donnent lieu à moins d'inquiétude, du point de vue sécurité, que les autres types de systèmes. Cela provient du fait que les systèmes de la défense sont protégés par une multitude de moyens comme la surveillance du personnel, l'installation d'enceintes en fils de fer barbelés, etc. On a tout intérêt, dans la plupart des cas, à doter d'une plus grande sécurité les banques de données, disons de la Croix bleue, que celles employées pour la défense."

Egalement au sujet de la sécurité, M. John Russell a fait remarquer que le contrôle des mots de passe et d'autres systèmes d'identification est une opération coûteuse qui prend

beaucoup de temps et qu'il ne faut pas mettre en vigueur trop vite. "Les législateurs devront par conséquent prévoir des délais statutaires suffisants entre la date de la demande et celle de la permission accordée pour accéder à une banque de données."

3. Moyens d'action

La suggestion la plus courante a été d'établir un organisme qui serait chargé de réglementer des systèmes d'information de type bien précis et de leur délivrer des licences. On n'a guère discuté sur la question de savoir si le même organisme devrait contrôler les systèmes d'information et leurs exploitants ou si on devrait avoir deux organismes séparés pour cette tâche. On a cependant beaucoup insisté sur le fait que les systèmes d'information exploités par le gouvernement (y compris ceux de la police) devraient être soumis au contrôle de l'organisme de réglementation. Certains délégués ont exprimé des doutes à ce sujet. L'un d'eux a dit péremptoirement: "Comment voulez-vous qu'un organisme du gouvernement puisse surveiller d'une manière impartiale et qui inspire confiance un autre organisme du gouvernement?" Cela s'est évidemment produit plusieurs fois au Canada et c'est peut-être ce qui a provoqué cette remarque!

Un argument contre le principe des licences (mais non contre les règlements gouvernementaux) a été avancé par Mr A.E. Ende, de la Federal Communications Commission. Il s'est dit plutôt en faveur de l'établissement de normes et du contrôle de leur application. Il a déclaré que les licences sont souvent délivrées en suivant des critères qui peuvent ne plus être valables en raison des progrès technologiques. Une fois adoptés évidemment, ces critères sont difficiles à changer. Par ailleurs, les personnes qui détiennent une licence y deviennent très attachées. Si on se contente d'établir des normes, on peut facilement les modifier selon les besoins et les publier, et ceux qui ne s'y conforment pas sont punis. Finalement, M. Ende a fait remarquer que la délivrance de licences est peut-être un moyen utile lorsqu'un gouvernement accorde des concessions pour l'utilisation de ressources rares (par exemple les fréquences de radiodiffusion), mais que cela ne s'applique pas dans le cas des banques de données.

De plus, l'idée d'établir un organisme de surveillance de la réglementation a reçu la faveur de beaucoup de délégués. Six groupes de travail ont discuté de la possibilité d'établir un ombudsman, un conseil ou un tribunal ayant un mandat déterminé. Son rôle consisterait à recommander l'adoption de règlements ou de lois, mais cet organisme n'aurait aucun pouvoir de réglementation ou de législation. Ce conseil pourrait également entendre les causes en dommages résultant des systèmes d'information, faire des recherches sur le perfectionnement des

banques de données, évaluer les normes professionnelles, etc. De telles propositions semblent indiquer un accord général sur la nécessité d'un organisme consultatif qui soit indépendant des autorités législatives et exécutives. Certains délégués ont suggéré que ce conseil soit formé de représentants de divers groupes des secteurs privé et public.

4. Note concernant la compétence législative

Le professeur J.M. Sharp a plaidé en faveur d'une compétence fédérale sur les systèmes d'information, surtout pour les raisons suivantes: "Je ne peux rien envisager de plus désagréable ou de plus intolérable que le fait qu'une province quelconque devienne le Las Vegas de l'informatique en battant ce qui serait le commode pavillon de Panama pour l'informatique, alors que les autres provinces auraient établi une réglementation sévère. A mon avis, cela pourrait facilement se produire si le gouvernement fédéral n'assumait pas le contrôle de l'informatique au Canada."

Selon M. Sharp, "il semble qu'il faudrait que la réglementation fédérale vise au moins les ordinateurs et les banques de données qui participent aux échanges interprovinciaux et internationaux de données sur la solvabilité, le commerce, etc."

M. Sharp a fait allusion à la doctrine du "Mouvement du commerce", à l'analogie avec les télécommunications qui est formulée dans la Loi de la Télésat Canada de 1969, au droit pénal et à la sécurité nationale. Il a cependant reconnu que pour les systèmes à l'intérieur des provinces, "une législation provinciale seulement (si possible uniforme) serait nécessaire. Peut-être qu'une analogie approximative pourrait être tirée des relations existant, d'une part, entre la Loi sur les stupéfiants et la Loi sur les aliments et drogues et, d'autre part, les lois provinciales relatives aux pharmacies. Dans une certaine mesure, ces lois se complètent. Il n'y a aucune raison pour ne pas mettre au point un système de lois fédérales et provinciales coordonnées pour les banques de données et pour les renseignements qu'elles contiennent."

Le Professeur Douglas A. Schmeiser, de la faculté de Droit de l'Université de la Saskatchewan, qui était président de la table ronde sur les moyens juridiques et administratifs propres à favoriser la réalisation des objectifs, trouve que "les arguments en faveur de la compétence fédérale dans le domaine de la vie privée ne sont guère frappants." Cependant, ni M. Schmeiser, ni M. Sheppard, qui était d'accord avec lui, n'ont donné d'autres précisions.

M. Sheppard a cependant déclaré que "les aspects constitutionnels du contrôle juridique des banques de données ne

sont pas aussi complexes qu'ils le paraissent. Il me semble fort douteux que le gouvernement fédéral puisse réclamer la compétence exclusive. En toute probabilité, et pour ne pas déroger à la bonne vieille tradition schizophrénique canadienne, la compétence sera partagée entre Ottawa et les provinces."

5. Considérations internationales

A certains égards, la discussion concernant la compétence législative à l'intérieur du Canada est un exercice vain, car on a reconnu lors de la conférence que le "Las Vegas" de l'industrie canadienne des banques de données pourrait fort bien être la ville de Las Vegas elle-même. Par suite des nombreux circuits de télécommunications reliant déjà le Canada et les Etats-Unis, il est pratiquement impossible d'arrêter tout passage de données à la frontière, si les exploitants des banques de données veulent qu'il en soit ainsi. Les lois canadiennes peuvent exiger que les données relatives aux Canadiens soient gardées au Canada, comme l'ont demandé certains délégués, mais il semblerait difficile d'empêcher quiconque est déterminé à le faire de garder aux Etats-Unis des copies de ces données.

Par conséquent, comme d'autres délégués l'ont suggéré et particulièrement M. Guy Braibant, du Conseil d'Etat de France, il y aurait lieu d'étudier les possibilités de coopération internationale. Comme M. Braibant l'a dit: "Si certains pays adoptaient une réglementation sévère alors que d'autres ne le feraient pas, avec les progrès des communications nous risquerions de voir certains pays constituer des refuges pour banques de données. Je crois qu'au cours de la prochaine décennie, les Nations Unies devront immanquablement envisager la création d'accords internationaux dans ce domaine, comme elles l'ont fait dans le domaine des télécommunications."

Les mesures internationales n'enlèvent évidemment pas le besoin de mesures au niveau national. Si le Canada ne prend pas de mesures intérieures, quelle que soit la tournure des négociations internationales, notre pays pourrait bien devenir l'un de ces refuges dont a parlé M. Braibant!

6. Conclusion

Les rapports de sept ateliers sur douze recommandent l'établissement d'un groupe spécial chargé d'étudier les mesures législatives qui pourraient être prises. Certains suggèrent un groupe constitué par des représentants du fédéral et des provinces, tandis que d'autres favorisent une représentation des secteurs public et privé. Un atelier a même soulevé l'idée d'un groupe très restreint d'experts qui seraient chargés d'étudier minutieusement les nombreuses questions soulevées lors de la conférence.

Ces propositions donnent peut-être une excellente idée de la conviction des délégués quant à l'urgence des mesures à prendre. La même conviction se retrouve dans cette déclaration de M. A.E. Gotlieb:

"Le fossé qui sépare les progrès technologiques et la réglementation ne doit plus s'élargir. Au contraire, des mesures décisives doivent être prises pour le combler rapidement. Les gouvernement fédéral, provinciaux et municipaux, les groupement d'avocats, les universités, les chercheurs, les savants et tous ceux qui s'intéressent à ces questions ont la responsabilité de proposer des solutions qui reconnaissent et protègent le droit à la vie privée des citoyens dans cette société nouvelle que nous promettent les ordinateurs et les télécommunications."

Annexe A

Définition de la vie privée

Tous les ateliers, sauf un qui n'a pas été très spécifique sur la question, ont discuté du droit à la vie privée. Ils sont presque tous tombés d'accord sur le fait que ce droit à la vie privée devrait être de plus en plus protégé, avec toutefois certaines réserves.

La plupart des ateliers ont éprouvé des difficultés lorsqu'il s'est agi de définir le concept de vie privée, et plusieurs d'entre eux ont évoqué la nécessité de considérer la notion de vie privée comme un concept juridique, et même d'élaborer une philosophie de la vie privée. Quelques ateliers ont douté que l'on puisse le faire dans un temps si court, et d'autres, estimant que ce concept variait selon les circonstances historiques et sociales, ont proposé de confier sa définition aux tribunaux.

Par ailleurs, d'autres ateliers sont arrivés à la conclusion que le droit à la vie privée devrait être inscrit dans la loi, et qu'il devrait y être conforme à la Déclaration universelle des droits de l'homme.

On a constaté une grande différence d'opinion sur la question de savoir si les ordinateurs entrent en ligne de compte dans la notion de la vie privée. Certains croient que les ordinateurs ont un effet direct sur la vie privée, tandis que d'autres sont persuadés que ces machines n'ont rien à voir avec la vie privée ou la liberté. D'autres encore pensent que les ordinateurs sont importants lorsqu'il s'agit de vie privée parce qu'ils ajoutent à ce problème.

Finalement, certains croient que la question de la vie privée ne devrait pas seulement viser les systèmes par ordinateur.

Liberté d'accès à l'information

Le droit à la vie privée comporte deux corollaires. On a généralement admis que les banques de données répondent à des besoins en matière de planification, de recherche et de commerce. De plus, dix des ateliers ont reconnu qu'il fallait assurer la liberté d'accès à l'information. On a considéré que cela était particulièrement important en ce qui concerne l'information gouvernementale, et une loi concernant la liberté de l'information, semblable à celle qui est en vigueur aux Etats-Unis, a semblé nécessaire à beaucoup.

Aspects techniques - Effet des ordinateurs sur la vie privée

On n'a pas été d'accord sur la question de savoir si les ordinateurs étaient directement reliés à la question de la violation de la vie privée des citoyens. L'opinion la plus répandue a été que l'ordinateur, qui permet de chercher plus rapidement dans des dossiers plus complets, avait de fait modifié la nature du problème de la vie privée. Cependant, l'ordinateur offre la possibilité d'effectuer des contrôles de sécurité qui sont bien plus efficaces que ceux des systèmes manuels.

Bien que certains mémoires aient fait allusion à un haut degré de sécurité dans les services de téléinformatique, on a estimé que la technologie actuelle ne permet pas de protéger pleinement ces systèmes. Le niveau de protection doit correspondre au type de données mises en mémoire dans les banques de données. La meilleure solution serait donc d'employer des systèmes différents pour les divers types de banques de données. A l'heure actuelle, le problème de la sécurité mis à part, il ne semble pas possible du point de vue technique de mettre en service une banque nationale de données qui desservirait un réseau unique. On pourrait peut-être employer à cette fin un réseau d'ordinateurs.

Groupe d'étude

Sept ateliers ont recommandé qu'un groupe d'étude soit formé. Trois de ces ateliers ont suggéré un groupe composé de représentants du fédéral et des provinces, tandis qu'un autre a préconisé un groupe de spécialistes en droit, informatique, sciences sociales, affaires et éducation ainsi que des représentants du gouvernement. Plusieurs fonctions ont été suggérées pour cet organisme: évaluation des lois et des méthodes actuellement en vigueur; enquête sur la divulgation des données personnelles; identification des problèmes spécifiques; définition de la vie privée, des banques de données, des systèmes d'information, etc.; étude des questions constitutionnelles et recommandations concernant les lignes de conduite et les lois à adopter. Certains ateliers ont insisté sur la nécessité de former ce groupe d'étude le plus tôt possible.

Conseil, tribunal, ou ombudsman

Six ateliers ont suggéré la formation d'un conseil qui n'aurait aucun pouvoir de réglementation ou de législation, mais qui pourrait faire les recommandations appropriées pour ce qui est des lois et des règlements.

Certains ont suggéré quelques fonctions précises:

- étudier les dommages spécifiques résultant du mauvais emploi de l'information;

- donner des conseils au sujet du développement possible des banques de données; faire des recherches sur la classification des données;
- entendre les plaintes;
- déterminer les normes professionnelles; étudier les genres de renseignements qui sont mémorisés et l'usage qu'on en fait;
- délivrer les licences aux banques de données; exiger que les exploitants déposent des rapports périodiques sur les méthodes utilisées pour les systèmes; exiger une permission préalable pour l'échange ou la vérification de données entre deux systèmes distincts.

On a suggéré des ombudsmen aux échelons fédéral et provincial. Le conseil ou le tribunal proposé devrait comprendre des représentants du gouvernement fédéral et des gouvernements provinciaux ainsi que des délégués de l'industrie (selon une proposition, la majorité des membres devrait provenir du secteur privé), des universitaires et des groupes comme les associations de consommateurs et les comités de citoyens. Il est à noter que la création d'un tel conseil ou tribunal est aussi considérée comme une mesure temporaire qui permettrait d'élaborer une législation, qui remplacerait les mesures législatives, ou encore comme un complément à une enquête du groupe d'étude.

Licences et reconnaissance professionnelle

Presque tous les ateliers ont recommandé qu'il y ait un processus de délivrance de licences ou de reconnaissance professionnelle. Cette exigence a été jugée nécessaire uniquement à des fins de contrôle. Les licences devraient être délivrées par un organisme indépendant et identifier le type de banque de données. On a suggéré que tous les types de banques de données personnelles aient une licence d'exploitation, dont la catégorie dépendrait du genre de renseignements qui y sont gardés. A cet égard, on a fait remarquer qu'une personne pourrait être identifiée même si son nom ne figurait pas dans le dossier.

Un atelier a suggéré qu'il fallait que les banques de données à téléaccès obtiennent une licence, car les problèmes de sécurité associés au partage du temps n'ont pas encore été résolus.

Un autre atelier a posé les questions suivantes:

- Est-il souhaitable de délivrer des licences?

- A qui devrait-on les délivrer:

- aux enquêteurs
- aux propriétaires de banques de données
- aux programmeurs?

D'une façon générale, des licences devront être délivrées aux personnes dont le travail est de nature confidentielle.

Lois et règlements

Quatre ateliers n'ont fait aucune suggestion précise quant aux lois. Cependant, l'un de ces ateliers a reconnu que le droit à la vie privée devait être protégé par la loi, et qu'il faudrait au moins mettre sur pied un organisme de réglementation.

Sept ateliers ont présenté des suggestions précises en vue d'une législation qui a été qualifiée du type "bikini", c'est-à-dire destinée à couvrir l'essentiel:

- a. protection de la vie privée des citoyens (six ateliers);
- b. protection assurée par une responsabilité civile en cas de dommage (trois ateliers); responsabilité criminelle et dédommagement (un atelier);
- c. droit à la vie privée accordé conformément à la Déclaration des droits de l'homme (deux ateliers);
- d. droit pour toute personne de consulter son dossier (deux ateliers);
- e. droit d'accès du particulier à son propre dossier devant être contrôlé par lui (deux ateliers).

Deux ateliers ont suggéré que les lois soient libellées de telle sorte qu'on puisse profiter de l'expérience et adopter ensuite en connaissance de cause des lois plus adaptées aux besoins. Un atelier a suggéré que cette législation essentielle devait être adoptée le plus tôt possible. Deux ateliers ont recommandé que la législation permette une plus grande liberté d'accès aux données gouvernementales.

Parmi les autres aspects de la législation envisagés par ces ateliers, on peut mentionner que les règlements adoptés devraient s'appliquer aux dossiers du gouvernement aussi bien qu'aux autres dossiers, et que les renseignements nécessaires au bien public devrait être clairement nommés dans la loi, qui

devrait aussi mentionner ceux à qui ils peuvent être révélés. Un atelier du même groupe a fait savoir que la législation fédérale était nécessaire à cause du problème des "refuges" et de la facilité de transmission des données.

L'Atelier n° 3 a porté beaucoup d'attention aux propositions de nature législative; même si certains points ont été couverts par d'autres, nous croyons qu'il vaut mieux consulter leur rapport que d'essayer de le résumer.

En tout, 8 ateliers sur 12 ont recommandé le recours à la législation. Aucun atelier ne semble avoir enregistré d'opposition à la législation. Un atelier a même suggéré d'adopter une législation dès que les renseignements nécessaires auront été obtenus, mais a mis en garde contre des mesures prises sans s'appuyer sur des données suffisantes.

Sanctions

Huit ateliers ont recommandé que des sanctions soient prévues en cas de négligence ou de mauvaise foi dans l'utilisation de l'information. Six d'entre eux ont fait une distinction entre les sanctions civiles et les sanctions criminelles. Dans le cas des sanctions civiles, tout abus devrait donner lieu à une poursuite en dommages et intérêts.

Un atelier a par ailleurs estimé que le transfert de renseignements d'une banque de données à une autre devrait être interdit. Un autre atelier a recommandé la création d'un fonds public pour indemniser des pertes personnelles lorsqu'un procès n'est pas possible.

Plusieurs commentaires ont été faits au sujet du rôle du gouvernement en matière de réunion des données:

- on n'a pas accordé suffisamment d'attention aux dossiers d'informatique du gouvernement; tout organisme de réglementation devrait être indépendant du gouvernement car celui-ci est propriétaire de très grands systèmes; en dehors de la sécurité nationale, le gouvernement devrait être soumis à tous les contrôles qui seront adoptés.
- selon deux ateliers, même les systèmes de la police devraient être contrôlés.

Questions internationales

Trois ateliers ont demandé que la législation assure que le contrôle des banques de données reste entre les mains des Canadiens, particulièrement lorsque ces banques contiennent des renseignements personnels au sujet des Canadiens. Un groupe a suggéré qu'on étudie les possibilités de coopération

internationale pour la protection de la vie privée des
particuliers.

Annexe BParticipants aux tables rondes et conférenciers

1. Vie privée et liberté de l'information en tant que concepts juridiques et sociaux

Président

M. John J. Deutsch,
Principal et vice-chancelier,
Université Queen's

M. A.E. Gotlieb,
Sous-ministre,
Ministère des Communications
Ottawa

Maître Claude-Armand Sheppard,
Etude Robinson, Sheppard
Drymer et Shapiro,
Montréal

Honorable John Turner,
Ministre de la Justice,
Ottawa

2. Banques de données: technologie et pratiques actuelles

Président

Pr Jacques Saint-Pierre,
Directeur du Centre de calcul,
Université de Montréal

M. R.F. Linden,
Ministère de l'Industrie et du Commerce,
Ottawa

M. T.J. VanderNoot,
Directeur général adjoint,
Développement et exploitation des systèmes,
Bureau fédéral de la statistique
Ottawa

M. M.T. Pearson,
Gérant général,
Associated Credit Bureaus of Canada

3. Banques de données: orientation et développement résultant des besoins et de la technologie

Président M. Louis Robichaud,
Directeur,
Centre de traitement de l'information
Université Laval

M. D.F. Parkhill,
Directeur général,
Politique, projets et programmes,
Ministère des Communications
Ottawa

M. B.B. Goodfellow,
Directeur,
Laboratoires IBM Canada

M. Willis H. Ware,
Rand Corporation,
Santa Monica
Californie

Conférencier
invité Honorable Eric Kierans,
Ministre des Communications

4. Objectifs à atteindre pour assurer la vie privée et la liberté de l'information dans les banques de données

Président M. T.B. Smith,
Section de la consultation et du droit
international,
Ministère de la Justice
Ottawa

Pr Calvin C. Gotlieb,
Directeur,
Institut d'informatique
Université de Toronto

Pr Hugh Lawford,
Département de droit,
Université Queen's

Pr Thomas L. McPhail,
Co-président,
Département des arts de communications
Collège Loyola

5. Moyens techniques et professionnels permettant d'atteindre les objectifs

Président Maître Guy Houle,
Services juridiques,
Bell Canada

M. Mers Kutt,
Président,
Consolidated Computer Services Ltd.

M. David F. Booth,
I.P. Sharp Associates Ltd.

M. J.M. Russell,
Vice-président,
Recherche et expansion
Systems Dimensions Ltd.

6. Moyens juridiques et administratifs permettant d'atteindre les objectifs

Président Pr. Douglas A. Schemiser,
Ecole de droit,
Université de la Saskatchewan

M. Paul Armer,
Directeur,
Centre de calcul
Université Standford

Maître Claude Frenette,
Vice-président,
Power Corporation of Canada Limited

Pr. J.M. Sharp,
Institut de recherches juridiques,
Faculté de droit
Université du Manitoba

Réunion de clôture
Instructions générales

Président Maître Jean Beetz,
Doyen de la Faculté de droit,
Université de Montréal

Rapporteurs M. Yves Legris,
Ministère des Communications

M. Leslie Mezei
Université de Toronto

Comité de la Conférence

Président de M. Richard Gwyn,
la conférence Ministère des Communications

Organisateur M. Calvin C. Goblief,
du programme Université de Toronto

Membres M. J. Ryan,
Ministère de la Justice

M. J. Crowson,
Ministère des Communications

M. D. Booth,
I.P. Sharp Associates Ltd.

Président du M. Hugh Lawford,
comité Université Queen's
d'organisation

Annexe CParticipants

MM. ABBEY, D.S.,
Ontario Institute for Studies in Education
Toronto

ADAMEK, P.,
Banque du Canada
Ottawa

ALBRECHT L.K.,
Royal Insurance Group
Toronto

ALLEN, R.E.,
Canadien Pacifique
Montréal

AMEY, G.X.,
Conseil de recherches pour la défense
Ottawa

ANDERSON, M.F.,
Simpsons-Sears Limited
Toronto

BALMER, D.,
Association canadienne des banquiers
Toronto

BAUDOT, J.,
Centre de calcul
Université de Montréal

BAXTER, D.C.,
Ministère des Approvisionnements et Services
Ottawa

BEAVIS, D.B.,
Bureau du Conseil Privé
Ottawa

BEETZ, J.,
Faculté de Droit
Université de Montréal

BEEZLEY, J.A.,
Affaires extérieures
Ottawa

BENETEAU, B.A.,
Québec - Téléphone
Rimouski

BERGERON, G.,
Ministère des Communications
Ottawa

BONYUN, D.A.,
Centre de calcul
Université Acadia

BOUWMAN, R.J.,
B.C. Telephone Company
Vancouver

BOWKER, W.,
Institute of Law, Research and Reform
Université de l'Alberta

BRAIBANT, G.,
Conseil d'Etat
France

BRAZEAU, J.,
Centre de sondage
Université de Montréal

BOOTH, D.F.,
I.P. Sharp Associates
Ottawa

BROWN, C.,
Bureau du Chef de l'Opposition,
Gouvernement de l'Ontario
Toronto

BRYSON, G.,
Alphatext Systems Limited
Ottawa

BURGER, A.F.,
Ministère des Finances
Ottawa

MME BURNHAM, M. Elizabeth,
The T. Eaton Company Limited
Toronto

- MM. BUTTERFIELD, F.J.,
Télécommunications du CN
Toronto
- CARON, Y.,
Montréal
- CARROLL, J.M.,
Département d'informatique
Université Western Ontario
- CARSS, T.O.,
Bell Canada
Montréal
- CHARLES, W.H.,
Ecole de droit
Université Dalhousie
- CHEETHAM, A.,
Ontario Credit Union League Ltd.
Toronto
- CLENNETT, M.C.,
Banque Royale du Canada
Montréal
- CLERMONT, M.,
Banque Canadienne Nationale
Montréal
- MME COOKE, Susan,
Credit Granters Association of Canada
Toronto
- MM. COOTE, G.F.,
Computer Data Processing Ltd.
Calgary
- COSTA, J.P.,
Délégation à l'informatique
Conseil d'Etat, France
- COTLER, I.,
Ministère de la Justice
Ottawa
- CROWSON, J.S.,
Ministère des Communications
Ottawa

DARLING, P.A.,
Centre de calcul
Université de Victoria

MME DESJARDINS, Alice,
Bureau de Conseil Privé
Ottawa

MM. DEUTSCH, J.J.,
Principal et vice-chancelier
Université Queen's

DOLAN, F.J.,
Centre de données
Université de Calgary

DORION, Juge G.,
Régie des services publics
Québec

ENDE, A.H.,
Federal Communications Commission
Etats-Unis

FIELD, F.W.,
Bell Canada
Montréal

FIERHELLER, G.A.,
Systems Dimensions Limited
Ottawa

FORGET, G.,
Centre de documentation
Université Laval

FOX, R.G.,
Centre de criminologie
Université de Toronto

FREEDMAN H.A.,
Bureau fédéral de la statistique
Ottawa

FUNK, J.A.,
Saskatchewan Telecommunications
Regina

GARDNER, Capt. M.T.,
Quartier général des Forces canadiennes
Ottawa

GALLOUEDEC-GENUYS, F.,
Centre national de la recherche scientifique
Paris

GIRARD, J.R.,
Ministère de l'Education
Québec

GLINSKI, G.S.,
Département d'électrotechnique
Université d'Ottawa

GORDON, H.P.,
Avocat,
Montréal

GRAHAM, Prof. J.W.,
Centre de calcul
Université de Waterloo

GOODFELLOW, B.B.,
IBM Canada
Toronto

GOTLIEB, A.E.,
Sous-ministre des Communications
Ottawa

Gotlieb, C.C.,
Institut d'informatique
Université de Toronto

GUTHRIE, A.D.,
Avocat,
Montréal

GWYN, R.,
Ministère des Communications
Ottawa

HANSEN, B.,
Committee of Presidents of
the Universities of Ontario
Toronto

HOLMLUND, B.A.,
Département d'informatique
Université de la Saskatchewan

HARVEY, L.,
Control Data Canada Limited
Montréal

HAYES, R.D.,
Ministère de la Justice
Ottawa

HEAP, F.K.,
Ministère des Approvisionnements et Services
Ottawa

HEENAN, T.F.,
B.C. Telephone Company
Vancouver

HILTON, D.A.,
Ministère des Communications
Ottawa

HOFLEY, B.C.,
Bureau du Solliciteur général
Ottawa

HOULE, G.,
Bell Canada
Montréal

HUGHES, C.J.,
Département de mathématiques
Université d'Ottawa

HOWARD, F.E.,
Ministère des Communications
Ottawa

MME IRON⁸SIDE, Diana J.,
The Ontario Institute for
Studies in Education
Toronto

MM. IEVERS, F.,
Ministère des Communications
Ottawa

IRWIN, J.W.,
Retail Council of Canada
Toronto

JONES, R.H.,
Gendarmerie royale du Canada
Ottawa

JENKINS, W.,
Centre de calcul
Université Queen's

KATZ, L.,
Département de physique
Université de la Saskatchewan

KAUFMAN, H.,
Conseil des sciences du Canada
Ottawa

KEECH, G.L.,
Centre d'informatique
Université McMaster

KENNEDY, G.H.,
Retail Credit Company of Canada Ltd.
Toronto

KIERANS, Honorable E.,
Ministre des Communications,
Ottawa

KING, E.E.R.,
Ministère des Communications
Ottawa

KINGSBURY, L.D.,
Imperial Oil Limited
Toronto

KOLTAI, S.K.,
Department of Treasury & Economics
Toronto

KUTT, M.,
Consolidated Computer Services Ltd.
Toronto

LAWFORD, H.,
Faculté de droit
Université Queen's

LEAL, H.A.,
Ontario Law Reform Commission
Toronto

LEDERMAN, W.R.,
Faculté de droit
Université Queen's

LEGARE, J.,
Département de démographie
Université de Montréal

LEGRIS, Y.,
Ministère des Communications
Ottawa

LIEBEL, P.,
Ministère des Communications
Ottawa

LINDEN, R.F.,
Ministère de l'Industrie et du Commerce
Ottawa

LATTA, K.,
Faculté de droit
Université Queen's

MACDONALD, J.B.,
Committee of Presidents of
Universities of Ontario
Toronto

MACNUTT, J.,
Ministère du Développement
Ile-du-Prince-Edouard

MANNING, E.G.,
Département d'informatique
Université de Waterloo

MARSH, A.,
Ecole de bibliothécaires
Université d'Ottawa

MASSICOTTE, J.,
Ministère des Communications
Ottawa

MCCLUNG, M.,
Secrétariat d'Etat
Ottawa

MCGEE, C.E.,
Ministère des Communications
Ottawa

MCINNES, G.A.,
Alphatext Systems Limited
Ottawa

MCPHAIL, T.L.,
Département des arts de communication
Collège Loyola, Montréal

MEZEI, L.,
Département d'informatique
Université de Toronto

MILNE, J.D.,
The Canada Life Assurance Company
Toronto

MURRAY, G.G.,
IBM Canada
Toronto

O'CONNELL, B.P.,
Département de recherches
Université McMaster

OGILVIE, J.C.,
Département de psychologie
Université de Toronto

O'REILLY, B.,
Ministère des Communications
Ottawa

PATENAUDE, P.,
Faculté de droit
Université de Sherbrooke

PATTERSON, Z.R.,
Ministère de l'Éducation de l'Ontario
Toronto

PEARSON, M.T.,
Associated Credit Bureaus of Canada
Toronto

PHARAND, D.,
Faculté de droit
Université d'Ottawa

POLLARD, W.I.,
London Life Insurance Company
London

POUNDER, D.W.,
Systems Dimensions Limited
Ottawa

RAYCRAFT, G.J.,
Ontario Credit Union League Limited
Toronto

REIMAN, R.I.,
Conseil du Trésor
Gouvernement de l'Ontario
Toronto

RIBLER, R.,
Computer Sciences Canada Limited
Toronto

RICHARDSON, L.E.,
T-Scan Limited
Toronto

ROBB, J.A.,
Avocat,
Montréal

ROBICHAUD, P.H.,
Centre de calcul
Université Laval

ROBINSON, P.,
Ministère de l'Agriculture
Ottawa

ROBSON, R.A.H.,
Département de sociologie et
d'anthropologie
Université de la Colombie-Britannique

RODGERS, I.,
Financial Post
Toronto

RUSSELL J.M.
Systems Dimensions Limited
Ottawa

RYAN, E.F.,
Ontario Law Reform Commission
Toronto

RYAN, J.W.,
Ministère de la Justice
Ottawa

SCHMEISER, D.A.,
Collège de droit
Université de la Saskatchewan

SCHNAITH, R.A.,
Univac
St. Paul (Minnesota)

SCOTT, D.B.,
Département d'informatique
Université de l'Alberta

SEAMAN, A.E.,
Ministère des Communications
Ottawa

SEDGWICK, G.G.,
Avocat,
Toronto

SHARP, I.P.,
I.P. Sharp Associates
Toronto

SHARP, J.M.,
Faculté de droit
Université du Manitoba

SHEPPARD, C.A.,
Avocat,
Montréal

SKELLY, S.,
Department of Attorney General
Winnipeg

SMITH, T.B.,
Ministère de la Justice
Ottawa

SOBERMAN, D.A.,
Faculté de droit
Université Queen's

SPEIGHT, J.A.,
CompuTech Consulting
Vancouver

SPICER, E.J.,
Bibliothèque du Parlement
Ottawa

MME STEWARD, Gail,
Conseil économique du Canada
Ottawa

MM. ST-PIERRE, J.,
Centre de calcul
Université de Montréal

TANNOCK, B.W.,
Shell Canada Limited
Toronto

TAPSELL, J.E.,
IBM Canada
Toronto

TATEISHI, A.T.,
Ministère des Approvisionnements
et Services
Ottawa

TAYLOR, G.F.,
Bell Canada
Montréal

TELLIER, P.M.,
Bureau du Conseil Privé
Ottawa

THOMAS, U.,
Secrétariat de l'OCDE
France

THOMSON, G.M.,
Gendarmerie royale du Canada
Ottawa

THOMPSON, G.B.,
Northern Electric Company
Ottawa

TOWERS, D.I.,

TRUDEL, J.P.,
Commission des écoles catholiques
de Montréal

TURNER, Honorable John,
Ministre de la Justice
Ottawa

VANDERNOOT, T.J.,
Bureau Fédéral de la statistique
Ottawa

WARE, W.H.,
The Rand Corporation
U.S.A.

WARREN, R.G.,
Ministère des Communications
Ottawa

WILLIAMS, I.,
Département de sociologie
Université Western Ontario

WILLIAMSON, D.,
Alberta Government Telephones
Edmonton

MME WILSON, Helen,
Ministère des Communications
Ottawa

MM. YEOMANS, D.R.,
Ministère des Approvisionnements et Services
Ottawa

ZEAMAN, Z.,
CRESIGU
Montréal

RENVOIS

1. La liste des participants à la conférence figure à l'Annexe C. Certains participants se sont plaints du fait que les jeunes, les consommateurs et le grand public n'étaient pas représentés.
2. La liste des déclarations écrites et des documents de base figure dans l'Annexe B. Le ministère des Communications fournira ces documents sur demande aux personnes intéressées.
3. Voir le rapport sommaire de la Conférence à l'Annexe A.
4. Le Professeur J.M. Carroll, de l'Université Western Ontario, a décrit ainsi le dossier des étudiants ontariens: "Il envahit leur vie privée beaucoup plus que ne le fait le dossier d'un criminel en instance de libération conditionnelle, d'un fonctionnaire s'occupant de questions très confidentielles ou d'un assisté social. L'étudiant doit révéler la langue qu'il parle chez lui, sa religion, la profession de son père, l'endroit où il fait ses devoirs, combien de temps il leur accorde et beaucoup d'autres détails sur sa vie "personnelle".
5. "Paradoxalement, toute intensification du secret gouvernemental compromet la vie privée des citoyens. Par contre, si on supprime le secret dans les organismes gouvernementaux et les autres institutions, les citoyens ont davantage de vie privée."

- Hugh Lawford,
Université Queen's
6. Voir la section 1, Vie privée et dignité.
7. Les remarques de M. Sheppard sont soutenues par la plupart des auteurs canadiens qui ont écrit sur le sujet. M. David Cornfield, dans la Faculty of Law Review de l'Université de Toronto, a dit: "quoique la vie privée soit partiellement protégée par les lois relatives à la violation de la propriété, aux atteintes à la tranquillité, à la négligence et aux droits d'auteur, aucun tribunal britannique n'a jamais donné de recours en ce qui concerne l'invasion en soi de la vie privée d'une personne, en dehors de son occupation d'une propriété ou de sa possession de biens personnels." Un autre auteur a écrit: "qu'il est assez sûr que le droit

britannique ne reconnaît pas le droit d'être laissé tranquille. La vie privée individuelle n'est pas protégée comme un droit, et il n'y a aucune obligation corrélative imposée aux autres personnes pour les empêcher de l'enfreindre."

Un récente exception se trouve dans l'affaire Robbins contre Radio-Canada, dans laquelle il a été jugé que Radio-Canada avait eu tort d'inviter les téléspectateurs d'une certaine émission à écrire ou à téléphoner pour "remonter le moral" d'un médecin qui avait envoyé une lettre à Radio-Canada pour se plaindre de cette émission. En se référant à la Section 1053 du Code civil, selon laquelle "toute personne capable de discerner le bien du mal est responsable des dommages causés par sa faute à un tiers, que ce soit par un acte positif, ou par imprudence, négligence ou incompetence", la Cour suprême du Québec a conclu que Radio-Canada avait commis une faute et était par conséquent responsable mais "qu'il n'était pas nécessaire de définir cette faute avec précision."

8. Westin, Privacy and Freedom. pp. 330-364
9. Pour obtenir plus de détails sur les entreprises canadiennes qui recueillent des renseignements personnels, voir Gibson, R.D. et J.M. Sharp, Privacy and Commercial Reporting Agencies, Legal Research Institute, Université du Manitoba, Winnipeg 1968.
10. Pour en savoir plus long sur le problème du "regroupement" et pour en avoir un exemple concret, voir au chapitre III au sujet de la R.H. Donnely.
11. Voir à l'Annexe IV le texte du projet de loi de M. Reid.
12. Cette expression a été employée par M. Parkhill pour décrire les énormes ensembles ordinateurs-communications, qui selon lui prendront la vedette dans un avenir rapproché. Voir plus loin son opinion à ce sujet.
13. Encore plus lorsqu'il existe une ligne de télécommunications entre le "client" et l'ordinateur.
14. Toutefois, un système est actuellement en voie de réalisation. La Gendarmerie a annoncé en septembre 1970 son intention de mettre en service une banque de données à accès direct qui contiendrait des renseignements au sujet des criminels et des voitures volées. Le système sera relié au NCIC (National Crime Information Centre) du FBI à Washington.

15. Les législateurs ou ceux qui rédigent les règlements auraient-ils intérêt à considérer l'ironie de l'exploitant d'un système d'information par ordinateur qui violerait la vie privée de ses employés afin de protéger celle de ses clients.
16. Une étude intitulée The Considerations of Data Security in a Computer Environment, et publiée par l'International Business Machines Corp. traite en profondeur des problèmes de sécurité.
17. Le mémoire de M. Sharp, qui est en fait un projet détaillé de mesures législatives, est reproduit intégralement à l'Annexe VI.
18. Mais cette proposition contient une embûche, à savoir que la banque de données, pour sa propre protection, devra tenir un registre des attestations ainsi fournies.

