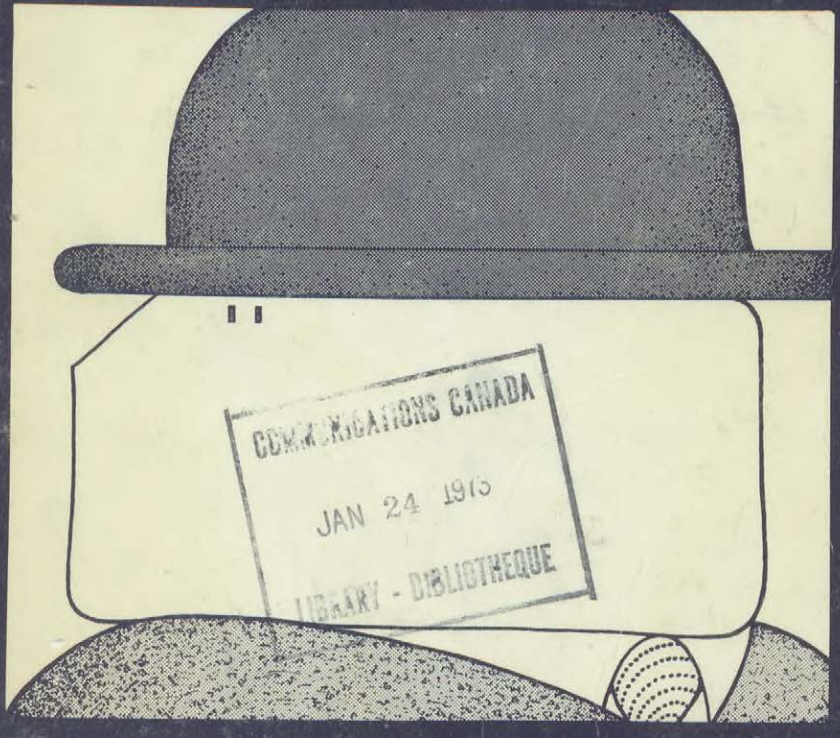
L'ORDINATEUR ET

LA VIE PRIVÉE



Rapport présenté par
le ministère des Communications et le ministère de la Justice

L'ORDINATEUR ET LA VIE PRIVÉE

2 L'ORDINATEUR ET

LA VIE PRIVÉE

1. Groupe d'étude sur l'ordinateur et la vie privée

Rapport du Groupe d'étude établi conjointement par
le ministère des Communications et le ministère de la Justice

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 $2.50 N° de catalogue Co21-3/1972F

Prix sujet à changement sans avis préalable

Information Canada
Ottawa, 1972

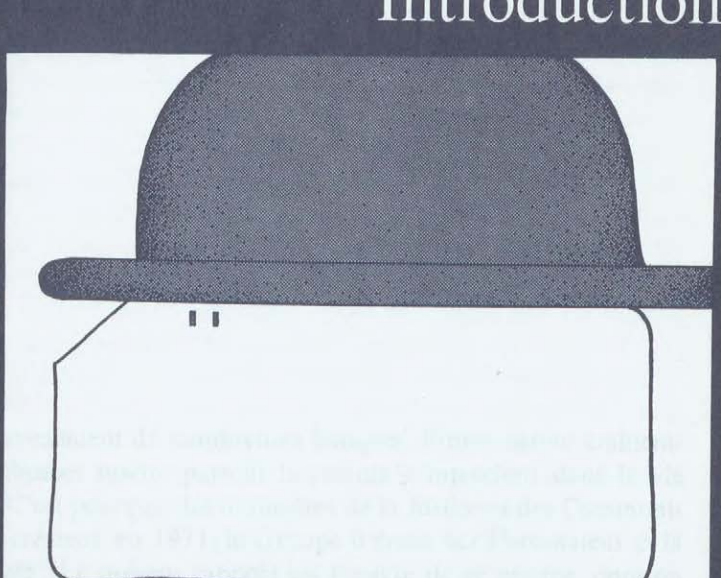
Conception graphique: John McIntyre
Hal Phillips

AVERTISSEMENT

Le présent rapport est l'œuvre de représentants des ministères fédéraux de la Justice et des Communications, et s'inspire des travaux d'experts. Les vues qui y sont exprimées ne représentent pas nécessairement celles du gouvernement canadien et il serait erroné d'y voir une indication de sa politique en ce domaine.

TABLE DES MATIÈRES

Introduction



Avant-propos

L'avènement de nombreuses banques d'information éminemment efficaces suscite partout la crainte d'intrusions dans la vie privée. C'est pourquoi les ministères de la Justice et des Communications créaient, en 1971, le Groupe d'étude sur l'ordinateur et la vie privée[1]. Le présent rapport est l'œuvre de ce groupe, dont on trouvera le mandat en appendice.

L'explication la plus simple de l'inquiétude qu'inspirent les systèmes d'information automatisés pour la vie privée en est aussi la plus évidente : les besoins croissants d'information – personnelle ou non – auxquels donnent lieu la complexité de la société actuelle et les attentes toujours plus grandes des individus et des groupes.

Les ordinateurs, notamment parce qu'ils sont dotés de mémoires prodigieuses, ont élargi à un point auparavant inimaginable les possibilités de collecte et de centralisation de renseignements personnels. Au siècle dernier, peu de gens étaient connus hors de leur entourage immédiat. Aujourd'hui, nous faisons tous l'objet de dossiers détaillés et complets : dossiers scolaires, de crédit, d'assistance sociale, d'assurances, d'impôt, de police. Se procurer un passeport ou une voiture, c'est laisser derrière soi une traînée de renseignements : de la naissance à la mort, nos traces se font de plus en plus marquées et nombreuses.

Jusqu'à récemment, le stockage et la diffusion de ces informations soulevaient peu d'inquiétude. Aux États-Unis, on en trouve la première manifestation aux audiences de la Chambre des représentants, en 1965, relatives au projet d'une banque d'information nationale. La réaction a été telle que le projet n'a pas eu de suite. Au Canada, rien de comparable n'est venu imposer le problème à l'attention générale. On note des manifestations occasionnelles : dans les journaux, à la Chambre des communes et dans les assemblées législatives où divers débats ont porté sur des propositions de loi. En mai 1970, à la *Queen's University*, une conférence (organisée conjointement par les ministères fédéraux de la Justice et des Communications et l'Association canadienne d'informatique) était consacrée au thème : « les ordinateurs, la vie privée et la liberté de l'information »[2]. C'est à la suite de cette conférence que devait être créé le Groupe d'étude sur l'ordinateur et la vie privée.

Nombre de pays ont mis sur pied des groupes d'étude analogues, notamment la Grande-Bretagne, la France, les États-Unis, la République fédérale d'Allemagne (où l'État de Hesse a été le premier à promulguer une loi sur les banques d'information) et la Suède — où le souci de la liberté de l'intimité remet en cause la liberté de l'information depuis longtemps jalousement préservée. La vaste enquête effectuée sous la direction du professeur Alan Westin, par l'Académie nationale des sciences des États-Unis, a particulièrement retenu notre attention. D'ailleurs, nous avons maintenu d'étroits contacts avec ce groupe tout au long de nos recherches[3].

Le Groupe d'étude a posé en principe qu'un examen des incidences de l'informatique sur la vie privée s'imposait actuellement ; que l'étude d'une question dont on discerne mal l'ampleur et la nature offrirait de meilleurs résultats si elle était confiée à des spécialistes. Vu le peu de temps dont nous disposions, l'étude visant à déterminer l'importance que les particuliers et la société attachent à la liberté de l'intimité a été menée de front avec celles portant essentiellement sur les faits et sur les aspects juridiques de la question. Les deux types d'études s'imposaient, si l'on voulait faire progresser un débat nourri jusqu'alors de considérations philosophiques et d'anecdotes touchant de mauvaises utilisations de données.

Notre plan de recherche comportait dix études principales : analyse multidimensionnelle de la nature de la vie privée ; diverses études sur les usages dans les organismes gouvernementaux, les établissements d'intérêt public et les entreprises de traitement de

données ; une étude prospective sur les développements technologiques ; diverses études sur les banques d'information réunissant des données statistiques, les problèmes de sécurité et les mesures de protection, la voie judiciaire, les mesures d'ordre administratif et réglementaire, l'autoréglementation, les questions constitutionnelles, les aspects internationaux. On trouvera à l'appendice, les titres des études ainsi que les noms de leurs auteurs.

De l'examen des pratiques informatiques se dégage un tableau révélateur. Il ne s'agit pas de faits sensationnels touchant une entreprise en particulier. La synthèse des résultats nous révèle l'existence d'un réseau complexe de collecte et de diffusion de renseignements reliant les administrations publiques et privées. En un mot, la collecte des informations personnelles atteint des proportions plus grandes que ne l'imaginaient la plupart des Canadiens, et leur diffusion se pratique à une plus grande échelle qu'on ne le suppose généralement. Rien n'indique non plus qu'il en sera autrement à l'avenir.

Les problèmes touchant la vie privée et l'information sont de deux ordres. D'une part, ceux qui sont reliés à l'exactitude des renseignements, au droit d'accès aux dossiers, au contrôle de la diffusion, aux normes de sécurité et autres questions de même nature. Nul besoin ici d'une analyse conceptuelle de base. L'essentiel est d'apprécier la nature et l'étendue exacte des problèmes et des solutions. Ainsi, on est généralement d'avis – quelle que soit la situation – que les renseignements consignés dans un dossier doivent être exacts, que la personne concernée a le droit de savoir, sauf impossibilité, à quelles fins les informations sont recueillies. On ne diffère d'opinion que sur la question de savoir où commencent les abus, et sur les mesures – législatives ou autres – à prendre pour les prévenir.

On se pose aussi des questions plus générales. Quelle relation y a-t-il entre l'information, la vie privée et le pouvoir politique ? L'utilisation présente et éventuelle de l'ordinateur marquera-t-elle la fin de l'individualité et accentuera-t-elle le conformisme ? La recherche de la liberté d'intimité face à l'information est-elle le signe d'une attitude antisociale ? Comment réalisera-t-on un juste équilibre entre les revendications en matière de vie privée et d'information – toutes deux parfaitement fondées mais parfois en opposition ?

Les enquêtes sur les pratiques informatiques et les études juridiques se relient aux questions du premier groupe. Par exemple, dans le premier cas, il s'agissait de déterminer les types de renseignements personnels que l'on recueille, les techniques de

stockage, les méthodes des exploitants de banques d'information. Pour ce qui est des études juridiques, il s'agissait d'établir quel accueil les tribunaux canadiens avaient fait aux recours contre des violations de la vie privée et quelle attention les corps législatifs canadiens ont accordée à cette question. De plus, les auteurs ont étudié diverses mesures tendant à assurer une meilleure protection à cet égard.

L'examen du second groupe de questions s'est révélé plus hésitant. En aucun cas, toutefois, ni pour ces dernières ni pour celles du premier groupe, nous avait-on demandé des solutions finales, ni avons-nous eu la prétention d'en offrir.

Ces dernières années, au cours des débats sur l'ordinateur et la vie privée, on a généralement considéré comme se rattachant à la vie privée l'éventail des intérêts, des exigences et des valeurs mis en cause par le stockage et le traitement de données. Nous tentons, dans le présent rapport, de clarifier ces notions en distinguant les valeurs que l'on peut justement relier à la vie privée, de celles qui – bien que soulevant des questions aussi pressantes, sinon davantage – se rapportent à d'autres problèmes, dont la réputation personnelle. Néanmoins une telle distinction n'a guère d'utilité lorsqu'on envisage des solutions aux problèmes de la collecte et du traitement de l'information. Ces solutions doivent être étudiées par rapport à l'éventail complet des atteintes effectives et virtuelles que comporterait l'exploitation des banques d'information, qu'il s'agisse de la vie privée ou des autres valeurs ou droits individuels.

Si le débat sur l'ordinateur et la vie privée déborde la question de la vie privée, il touche également bien d'autres domaines que celui de l'ordinateur. Comme l'indiquent les réponses au questionnaire distribué par le Groupe d'étude, les trois quarts environ des fichiers automatisés contenant des données personnelles s'appuient sur des fichiers manuels, lesquels portent de façon générale sur les informations les plus délicates. Il est probable toutefois que les progrès technologiques entraîneront l'automatisation de la plupart des fichiers, quels que soient les types d'information qu'ils contiennent. Dans le présent rapport, l'expression « système d'information » désigne donc les systèmes automatisés ou manuels.

Dernier mot d'explication, notre groupe se composait de fonctionnaires et de spécialistes de l'extérieur. Notre mission consistait à recueillir et à analyser les renseignements sur les systèmes d'information présents et prévisibles contenant des données sur des personnes identifiables et à faire l'étude des diverses mesures propres à assurer le respect de la vie privée et des

valeurs qui s'y rattachent. Le Groupe d'étude a pris connaissance, notamment par les media, d'allégations d'intrusions dans la vie privée, mais il n'en a pas examiné le bien-fondé.

Membres et collaborateurs du Groupe d'étude :

Comité de direction :
A. E. Gotlieb, Sous-ministre, Communications
G. V. La Forest, C.R., Sous-procureur général adjoint, Justice
R. J. Gwyn, Directeur général, planification de l'environnement, Communications
E. R. Olson, C.R., Directeur, recherche et planification juridiques, Justice.

Directeurs associés :
R. J. Gwyn, E. R. Olson

Principaux délégués des ministères :
Ann Johnstone, Justice
K. Katz, Communications

Conseillers :
J. Baudot, Université de Montréal
J. Boucher, Université de Montréal
J. Carroll, Université « Western Ontario »
C. M. Dalfen, Directeur, services juridiques, ministère des Communications
C. Fabien, Université de Montréal
H. S. Gellman, Président, DCF Systems Ltd., Toronto
C. C. Gotlieb, Université de Toronto
P. Hume, Université de Toronto
F. J. E. Jordan, ministère de la Justice
Carol Kirsh, Conseiller, Toronto
J. Madden, Groupe d'étude sur la téléinformatique au Canada, Communications
J. Sharp, Université du Manitoba
S. Usprich, Université « Western Ontario »
P. Vivian, Université « Western Ontario »
D. Weisstub, Université York
J. Williams, Université de l'Alberta
J. I. Williams, Université « Western Ontario »

Coordonnateur de la rédaction :
C. M. Dalfen

Rédaction :
A. Johnstone
J. Madden

La version française a été établie sous la direction de Fernand Doré

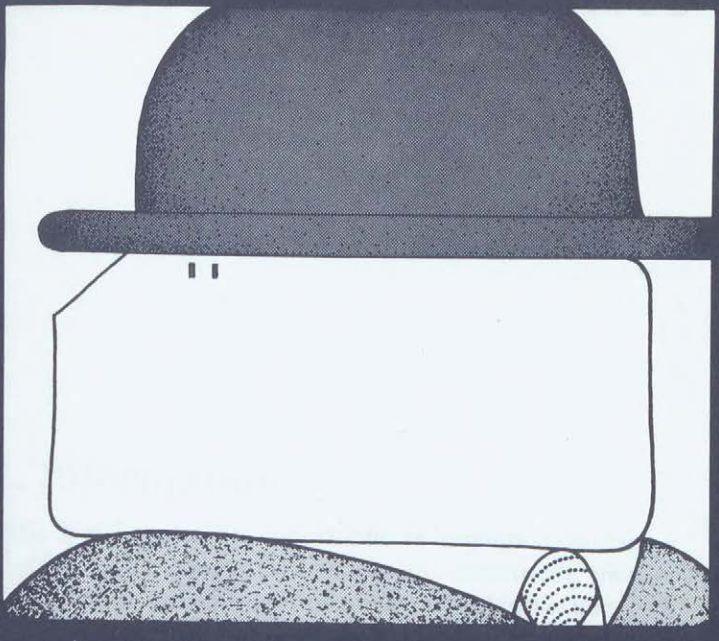
Chef de la publication :
Bette Byers

[1] À l'origine le mandat du Groupe d'étude sur la téléinformatique au Canada, créé le 1er novembre 1970 et dont le rapport a été rendu public le 3 août 1972, englobait l'examen des questions touchant la vie privée. On devait se rendre compte par la suite, en raison de l'ampleur et de la complexité du problème, de la nécessité d'en confier l'examen à un groupe d'étude distinct.

[2] Ministère des Communications, *Étude de la Télécommission 5(b)*, Ottawa, Information Canada, mai 1971.

[3] On trouvera à l'appendice la liste des études analogues effectuées à l'étranger.

Première partie



Champ et importance de la question

Chapitre premier
L'information et la vie privée

1. L'information

Depuis le début de l'ère industrielle et toujours davantage à l'époque plus complexe de la civilisation post-industrielle, tous les types d'information servent de fondement à la planification, à la recherche, à l'action des gouvernements et des universités, aux affaires et à presque toutes les formes d'activité. Individus, groupes et associations puisent de l'information dans le passé, à l'étranger, et s'informent mutuellement. Leurs systèmes absorbent un flot constant de données, les traitent, puis les diffusent, souvent après un cycle complet d'altérations et de transformations. L'appétit est grand : toutes les informations sont dévorées indistinctement et implacablement.

L'ordinateur est un outil qui sert au traitement de l'information. Sa capacité immensément supérieure à celle des systèmes manuels permet de traiter, d'assembler, de stocker et d'extraire des quantités énormes de données. Il centralise cette information dans des banques électroniques. Il surpasse la mémoire humaine en ce qu'il permet l'exploitation immédiate de données aussi diverses qu'innombrables. De nouveaux systèmes à mémoire prodigieuse

peuvent stocker plus de 100 milliards de caractères au coût d'environ 1¢ par mille. On travaille actuellement à mettre au point des techniques pour le traitement efficace de ces masses d'information et en même temps, grâce à des innovations technologiques, on perfectionne les postes terminaux des utilisateurs, on élabore des programmeries plus souples et plus générales et on étend la puissance des ordinateurs en y reliant les réseaux de télécommunication. En bref, la capacité qu'ont les systèmes informatiques de fournir de l'information à une rapidité et avec une efficacité sans pareilles va continuer de suivre une progression géométrique.

Leurs avantages sont donc immenses, notamment dans la planification et l'affectation des ressources, mais aussi pour assurer un accroissement d'efficacité dans les divers types d'activité. Presque tout ce que l'on fait, depuis la mesure du degré de pollution jusqu'à la gestion d'un programme d'assistance sociale, doit se fonder sur une information exacte et accessible touchant les gens et les choses. Sans information, le débat et l'analyse politiques sont appauvris : l'information confirme ou infirme le caractère discriminatoire des politiques d'embauche d'un établissement, le fait qu'un trop grand nombre de jeunes convoitent un nombre relativement restreint d'emplois, ou que les vieillards ne reçoivent pas les soins médicaux dont ils ont besoin.

Les immenses possibilités technologiques des systèmes d'information automatisés menacent toutefois certaines valeurs qui tiennent à l'essence même de la vie humaine comme nous la concevons, la vie privée, par exemple.

La société en vient rapidement à reconnaître les bienfaits indiscutables des systèmes d'information automatisés et à s'en prévaloir, comme en témoigne le prodigieux développement des ordinateurs de tous genres. Elle se rend moins bien compte, toutefois, de ses effets possibles sur les valeurs humaines. Le Groupe d'étude s'est donc attaché tout spécialement à ces valeurs et aux répercussions que peuvent avoir sur elles les systèmes d'information automatisés.

2. La vie privée et les valeurs sociales

La notion de vie privée est très confuse, elle comporte des aspects d'une grande complexité auxquels se mêle souvent de la subjectivité. L'expression « *droit* à la vie privée » est souvent

utilisée, mais il n'existe pas de définition juridique, ni même sociale, de ce droit, et toute discussion sur le sujet fait inévitablement ressortir une analogie aussi bien que des divergences avec les notions de liberté, de confiance, de pouvoir, de liberté d'accès à l'information.

La vie privée ne peut se ramener à une notion simple. C'est une constellation de valeurs concordantes et opposées, de droits solidaires et antagonistes, d'intérêts communs et contraires. Bien plus, cette constellation évolue avec le temps et varie d'un milieu culturel à un autre.

Bien sûr, ce sont surtout les individus qui revendiquent le droit à la vie privée. Dans des sociétés organiques comme celles du moyen âge, où l'on se souciait avant tout de la cohésion sociale et des besoins de la collectivité, il n'était guère permis aux individus de se tenir à l'écart, sauf aux moines ou aux mystiques. On aurait considéré comme antisociale sinon hérétique toute prétention à une identité indépendante de la seigneurie, de la corporation ou de l'église. Dans la société rurale qu'a connue l'Amérique du Nord jusqu'à une époque relativement récente, toute recherche d'isolement au-delà de celui qu'imposaient le milieu et le mode de vie aurait sans doute été jugée excentrique ou même hostile à la société et dangereuse dans les situations critiques. Et pourtant, ces sociétés rurales avaient un appétit sans borne pour les racontars, les « secrets » de chacun étaient souvent connus de tous.

La revendication du droit à la vie privée, sous sa forme actuelle, est donc un phénomène propre à l'ère industrielle et post-industrielle, où les nécessités de la vie urbaine conduisent à une conception atomique ou parcellaire de la société au lieu de l'image organique qu'on s'en faisait dans le passé. En quittant la campagne pour la ville, on échangeait autrefois l'isolement physique contre l'anonymat, mais l'échange perd progressivement de sa valeur à mesure que l'anonymat est compromis par la multiplication des systèmes et des réseaux d'information et que la solitude dans les villes n'existe à peu près plus. Le processus d'information se déroule d'ailleurs dans une seule direction : les administrations en connaissent davantage sur l'individu, mais l'individu n'en sait pas plus sur elles, ni même sur l'information qu'elles possèdent à son sujet.

Dans toute société, les phénomènes sociaux et politiques et les voies judiciaires mettent constamment en balance les exigences touchant à la vie privée avec d'autres valeurs. La sécurité et le bien-être de la collectivité et de ses institutions tendent à prévaloir sur le besoin d'intimité. Ainsi, les exigences du fisc et de la perception des

impôts l'emportent sur la volonté du contribuable de refuser toute information sur son revenu. La reconnaissance du droit à la vie privée par une société donnée dépend des idées et de la politique de l'époque. Il est possible qu'à une époque donnée certains droits soient reconnus par la loi (p. ex., le droit à la vie privée en ce qui concerne la plupart des activités qu'on exerce chez soi); que d'autres fassent l'objet de débats publics et officiels sans qu'on puisse encore les faire valoir en justice, et que d'autres enfin soient considérés comme inacceptables (p. ex., le droit de ne pas fournir à l'État les données relatives à son revenu personnel).

Les revendications relatives au droit à la vie privée ne s'inscrivent pas toutes dans un ensemble de valeurs et d'intérêts correspondant à une notion juste de la vie privée, même si, subjectivement, certaines d'entre elles s'en rapprochent. Revendiquer l'accès à une information personnelle destinée à d'autres équivaudrait plutôt à demander un nouveau partage du pouvoir politique (en neutralisant les répercussions d'une information virtuellement préjudiciable) ou à protester contre le gigantisme, la technocratie, l'impersonnalité qu'à réclamer le droit à la vie privée. Et les arguments invoquant la fausseté des informations n'ont pas, à proprement parler, de rapport avec la vie privée mais tiennent plutôt à la diffamation et aux autres atteintes à la réputation.

Malgré la fluidité des valeurs, le déplacement des intérêts et la variabilité des revendications, il est néanmoins possible d'isoler un certain nombre de constantes dans ce que l'on entend par vie privée et de définir les caractéristiques générales des valeurs que cherchent à protéger ceux qui prétendent qu'il y a eu intrusion dans leur vie privée.

3. La notion de vie privée

Les revendications en matière de vie privée peuvent se répartir en trois grandes catégories, selon qu'elles intéressent la propriété, la personne ou l'information. Ces trois catégories ont ceci de commun qu'elles obéissent à une force d'attraction qui en fait une constellation, à un principe voulant que dans certains domaines — considérés physiquement et psychologiquement — l'individu puisse, du fait de son existence propre, exiger qu'on le laisse agir à sa guise. Cette notion du droit d'agir à sa guise se justifie peut-être par les usages que l'individu peut faire de sa vie privée — jouissance d'autres libertés, satisfaction d'autres besoins humains, poursuite d'objectifs sociaux légitimes. Mais là n'est pas la question. Le point essentiel est que ces sphères ou domaines de la

vie privée sont importants, qu'ils sont indispensables au bien-être de l'individu (et, en fin de compte, au bon ordre de la société), indépendamment de l'usage qui en est fait. Le propre du régime totalitaire est de s'ingérer dans ces domaines, ce dont Orwell donne un exemple presque parfait dans *1984*.

a. Vie privée au sens spatial

Le droit à la vie privée considéré au sens spatial ou territorial se rattache, théoriquement aussi bien que juridiquement et historiquement, à la propriété. Il est un domaine physique à l'intérieur duquel le droit d'être seul et tranquille est non seulement revendiqué, mais aussi reconnu. L'homme est maître en sa maison. Il peut, chez lui, se protéger contre les intrus, les mauvaises odeurs, le bruit, les curieux. Personne n'y peut entrer sans sa permission, à moins d'être porteur d'un mandat en bonne et due forme.

b. Vie privée de la personne

Considéré dans un deuxième sens, le droit à la vie privée est protégé par des lois qui garantissent la liberté de mouvement et d'expression, interdisent la violence physique et imposent des restrictions à la perquisition et à l'arrestation sans mandat. Cette notion est également spatiale en ce sens qu'elle suppose la personne physique entourée d'une aura qui la protège. Contrairement à la propriété, cependant, cet « espace personnel » n'est pas délimité par des murs ou des enclos, mais par des lois et des valeurs sociales. La vie privée ne s'entend pas ici qu'au sens physique, car il s'agit surtout de sauvegarder la dignité de la personne humaine. La personne est moins protégée contre la perquisition en soi (la loi offre d'autres moyens de protection physique) qu'elle ne l'est contre l'affront, l'intrusion morale qu'elle représente.

c. Vie privée et information

La troisième catégorie de droits à la vie privée présentait un intérêt tout particulier pour le Groupe d'étude. Elle se fonde essentiellement sur une conception de la dignité et de l'intégrité de l'individu considérées en fonction de l'information de caractère personnel.

Cette conception de la vie privée découle du postulat selon lequel l'information de caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend. Et cela sans tenir compte de l'exactitude avec laquelle l'information

peut être subséquemment transmise, ni du préjudice qu'elle pourrait causer à l'individu dans sa réputation, ses biens ou son avenir ; évidemment, seules les circonstances permettent de déterminer le caractère préjudiciable d'une information. En raison de certaines valeurs sociales, il peut être nécessaire que l'individu fournisse des informations à une autorité compétente dans certaines circonstances (p. ex., à l'occasion d'un recensement). Il arrive que l'individu communique librement des informations pour obtenir certains avantages (p. ex., à un établissement de crédit pour obtenir un prêt, à son avocat pour gagner un procès, à son confesseur pour mériter le salut). Il peut aussi en faire part spontanément à ses intimes. En principe, il a cependant intérêt à savoir quel sort sera fait à ces informations, à en contrôler l'accès.

Au-delà de l'accès d'une première personne à une information de caractère personnel, l'individu a intérêt à savoir si et comment cette information sera transmise à des tiers et au public en général. Cela est particulièrement important lorsque l'information n'émane pas de l'intéressé : numéro de son passeport, numéro d'immatriculation de sa voiture. Dans ces deux cas, l'autorité émettrice a évidemment la haute main sur l'information, mais l'individu a quand même intérêt à en contrôler toute communication ultérieure.

Théoriquement, s'il y a intérêt à contrôler l'accès à l'information personnelle, ce n'est pas en raison de la souffrance morale ou du préjudice pécuniaire que la communication ou la publication sont de nature à causer. La vie privée de l'individu est « violée » chaque fois qu'une nouvelle personne prend connaissance de l'information. À mesure qu'une information de plus en plus abondante sur son état civil, ses habitudes, sa situation pécuniaire est communiquée à un nombre croissant de personnes, son autonomie est amoindrie d'autant, sa personalité est dévoilée, sa vie privée subit de nouvelles intrusions. L'individu qui fait valoir son droit à la vie privée demande aussi que l'information personnelle ne lui soit pas arrachée (perquisition, aveux forcés), qu'elle ne soit pas recueillie à son insu (écoute au téléphone ou aux portes), publiée sans son autorisation ni même communiquée à des tiers sans son consentement.

À l'analyse, l'intrusion dans la vie privée peut donc se produire de deux manières. D'abord au moment où un renseignement personnel est porté à la connaissance d'autrui. Il n'y aurait cependant pas d'intrusion si le renseignement était communiqué volontairement, sous le sceau du secret, par exemple au conjoint, à l'avocat ou au confesseur de l'intéressé. Pour qu'il y ait intrusion, il doit y avoir indiscrétion abusive. La deuxième forme d'intrusion se

produit lorsque le renseignement est transmis à un tiers ou qu'il est rendu public. Ici encore, il n'y a pas d'intrusion si l'intéressé donne le renseignement en toute liberté, sachant qu'il peut être publié.

4. Systèmes d'information et vie privée

Les deux cas où la vie privée est mise en cause dans l'exploitation des systèmes d'information correspondent à deux stades distincts du traitement de l'information. Au stade de la collecte des données, des organismes tentent d'acquérir sur l'individu des informations qui pourraient leur être utiles. C'est le premier processus d'appréhension des faits, même si les organismes glanent ces informations chez des tiers, des voisins potiniers, par exemple, et reçoivent par conséquent des informations de seconde main. Lorsqu'à leur tour ces organismes répandent l'information ou la communiquent intentionnellement ou indirectement à des tiers, c'est le deuxième cas d'atteinte virtuelle à la vie privée, comme d'ailleurs lorsqu'une fuite se produit parce que les techniques de sécurité du système ne sont pas au point. Il existe une grande diversité d'opinions quant à la légitimité des intérêts et des droits individuels mis en cause aux deux stades du traitement de l'information. Quelques-uns de ces droits sont entièrement ou partiellement reconnus par la loi. La Loi sur la radio interdit l'usage et la diffusion d'information obtenue par le captage non autorisé de messages radio. Au début de 1972, le Parlement a été saisi d'un projet de loi interdisant les tables d'écoute. Beaucoup d'autres droits, cependant, sont revendiqués et, dans certains cas, discutés publiquement alors que dans d'autres cas les revendications n'ont pas encore été formulées.

Les systèmes d'information soulèvent non seulement des questions touchant directement la vie privée, mais aussi de nombreux problèmes connexes. Certes ceux-ci se présentent aussi dans les systèmes manuels, mais l'ordinateur – par sa rapidité, sa capacité de stockage et sa mémoire à peu près infaillible – est de nature à les amplifier ou du moins à les mettre en évidence. Cet outil, que l'on peut programmer par télécommunication, permet d'établir des fiches personnelles (en quantités variables mais presque illimitées), de les stocker, de les extraire et de les transmettre, souvent sans le consentement et à l'insu de l'intéressé ; de centraliser, mettre en corrélation, puis réaménager des éléments d'information disparates de façon peut-être préjudiciable ; de

cumuler les erreurs et d'en exacerber les conséquences. On ne peut plus compter sur l'oubli que permettaient les limites de la mémoire humaine. Ainsi se posent les questions relatives à la vie privée et elles deviennent plus brûlantes à mesure que s'accroît le nombre de fiches personnelles dans les domaines les plus divers : de l'éducation au crédit, des prestations sociales aux assurances, des impôts au casier judiciaire.

Le Groupe d'étude a tenu à examiner les activités et les pratiques des informaticiens pouvant faire peser une menace ou influer sur la vie privée. Au stade du stockage et du traitement, il s'est attaché à la nature et aux types de données ; au réaménagement, à la fusion et à la contre-vérification ; au degré d'exactitude ; aux techniques de sécurité et à leur efficacité ; à la connaissance qu'a l'intéressé du fait que l'information est enregistrée et aux moyens qu'il aurait de s'en rendre compte ; enfin, aux possibilités qui lui sont offertes de se renseigner sur le contenu des fiches.

Au stade de la diffusion des données, le Groupe d'étude a fait porter son examen sur les questions suivantes : à qui telle information est-elle communiquée, dans quelles conditions et qu'en sait l'intéressé.

Le Groupe d'étude a aussi considéré certaines questions normatives que soulèvent les systèmes d'information. Il a posé, entre autres, les questions suivantes :

1. Dans quelles conditions l'intéressé devrait-il avoir accès aux fiches personnelles ?
2. Devrait-il avoir le droit de biffer, corriger ou compléter les renseignements que contiennent ces fiches ?
3. Dans quelle mesure pourrait-on raisonnablement exiger que l'information personnelle soit protégée contre l'indiscrétion ou la divulgation accidentelle ?
4. Quels sont les droits de l'individu relativement à la diffusion de l'information portée sur ses fiches ? Devrait-il être informé d'avance de la diffusion, ou être avisé (par un contrôle) de tous les usages qui en sont faits ?
5. Quelles sont les responsabilités des organismes détenteurs des fiches en matière de fusion et de diffusion des données personnelles ?
6. Le stockage de données personnelles hors du Canada peut-il être une source d'inquiétude pour l'individu ?
7. Dans quelle mesure l'organisme qui possède des données personnelles devrait-il être tenu responsable de leur exactitude ?

8. Devrait-il y avoir des conventions ou des règles concernant les types d'information personnelle que peuvent conserver les établissements ?

Les systèmes d'information, automatisés ou non, ne sont pas en eux-mêmes capables d'intrusion dans la vie privée, mais leur utilisation y conduit presque infailliblement. Le Groupe d'étude a cherché à mesurer l'étendue de cette intrusion, à en déterminer les limites acceptables compte tenu des besoins croissants de connaissance et d'efficacité et à préciser les garanties que l'individu serait en droit d'attendre relativement à l'élaboration et à l'exploitation des systèmes d'information automatisés.

5. La vie privée, besoin humain

La question de savoir si la vie privée répond à un besoin inné de l'homme a été posée par de nombreux auteurs. Westin, dans son ouvrage intitulé *Privacy and Freedom*, passe en revue la bibliographie du comportement et de l'anthropologie espérant y trouver une explication naturelle ou héréditaire de ce besoin. Les constatations sont convaincantes quant au besoin de vie privée au sens spatial, mais elles le sont moins en matière d'information.

L'instinct de l'habitat chez les animaux se retrouve dans les fiefs sous le régime féodal et dans l'évolution du droit personnel et du droit de propriété. Envisagé en fonction de la survivance de l'espèce, l'instinct de l'habitat trouve une explication logique. Pour ce qui est de la « spatialité » de l'information, cependant, les études anthropologiques de différentes tribus et civilisations ont révélé une variété de coutumes et de pratiques. Même dans le monde occidental actuel, nous avons l'exemple de la Suède où presque toutes les archives gouvernementales, y compris les déclarations d'impôt, sont, de par la loi, du domaine public, alors que d'autres pays, dont le Canada, imposent des peines sévères pour la divulgation de la même information, sauf dans des circonstances bien précises.

Si on considère les coutumes de différentes sociétés, qui reflètent des situations et des traditions toujours changeantes, on se rend compte que seule une étude plus poussée des relations humaines permettra de découvrir les racines de cette constante revendication du droit à la vie privée en matière d'information.

Dans son analyse du besoin humain de vie privée, Westin distingue quatre composantes. Ce sont : *la solitude* – pour que l'homme puisse réfléchir sur ce qui lui arrive ; *l'intimité* avec la famille et les amis – pour permettre des relations plus étroites, plus

attachantes ; *l'anonymat* – pour permettre à l'homme d'exister en dehors du milieu ou il évolue ; et *la distance* – pour qu'il puisse suspendre les communications quand il en éprouve le besoin.

De ces quatre composantes, c'est l'anonymat qui est le plus compromis par l'absence de vie privée en matière d'information. Mais le mot anonymat ne recouvre pas entièrement le besoin qu'éprouve l'intéressé de rester maître de l'information pour s'assurer qu'elle est communiquée d'une manière restreinte et sélective. Il serait peut-être plus exact d'y voir un aspect de la distance, qui consiste à soustraire une partie de soi-même à la communication. Ce besoin tient presque certainement à un désir de faire impression en communiquant un choix soigneusement étudié d'informations personnelles. Avec certains amis ou avec de parfaits étrangers, cette façade tombe parfois, mais la soif d'anonymat partiel est vive chez la plupart des humains. Un auteur[1] a résumé ainsi sa pensée à cet égard :

> « La vie quotidienne est donc constamment partagée entre la candeur et la ruse, entre l'épanchement et la circonspection, entre le désir d'embrasser l'univers et l'envie de nous soustraire aux pressions du groupe. Aussi faut-il, pour conserver notre identité, savoir nous tenir à l'écart aussi bien que fraterniser. »

Dans un monde de parfaite cohésion sociale et de confiance mutuelle, la protection de la vie privée ne serait peut-être pas nécessaire. Là où il n'y a pas d'antagonisme, le bonheur total résulte de la parfaite harmonie des parties. Dans *Brave New World*, Aldous Huxley donnait une vision de cette utopie. L'harmonie et le bonheur régnaient, mais il manquait une dimension importante. L'homme avait perdu la faculté de prendre une mauvaise décision dans un monde programmé et, du même coup, il avait perdu son identité, son individualité.

La centralisation et le traitement de grandes quantités de données personnelles constitue également une menace pour l'individualité. Cette menace réside dans le conformisme auquel l'individu est amené par la certitude que son dossier existe et grossit, et par l'incertitude quant à son contenu et aux usages qui en seront faits. Voici ce qu'en dit Westin :

> « Si on était averti des usages possibles de la fiche, on se comporterait en conséquence et on aurait moins de liberté d'action et d'expression. On ne s'inquiéterait pas que de la fiche, mais aussi de l'effet qu'elle pourrait produire auprès des autorités... »

6. L'ordinateur et le pouvoir

Outre les valeurs individuelles en jeu et indépendamment du mandat qui a été confié au Groupe d'étude, l'ordinateur soulève d'importantes questions politiques qui commencent seulement à être débattues publiquement. L'ordinateur est non seulement un outil servant à traiter des masses d'information, mais il est devenu un dispositif capable de concentrer des pouvoirs immenses entre les mains des informaticiens et de ceux qui contrôlent les systèmes d'information. Il peut être particulièrement redoutable dans les administrations publiques et privées. À ce propos, Michael Harrington[2] a écrit :

> « Dans une société moderne, l'administration est le seul moyen de coordonner les fonctions complexes de l'économie et c'est pourquoi on ne peut la répudier en la maudissant. Mais elle constitue aussi un énorme potentiel de puissance arbitraire, impersonnelle qui plie, courbe, façonne et mutile les individus tout en gardant intactes les cartes I.B.M. »

Jusqu'ici l'ordinateur ne traite que l'information enregistrée et il n'a pas encore appris à pénétrer dans l'esprit, dans les pensées intimes de l'homme, mais cela ne veut pas dire qu'il n'y parviendra jamais. Il paraît probable que les chercheurs inventeront des techniques pour obtenir un « signalement psychologique » en assemblant des informations sur les lectures, le milieu familial, la formation, etc., un peu comme le signalement d'un pirate de l'air dont se servent les compagnies d'aviation.

Les romans de science-fiction abondent en histoires d'ordinateurs qui surpassent l'intelligence de l'homme et finissent par conquérir le monde. D'autres, moins dramatiques mais tout aussi troublantes, présentent des hommes qui, à l'aide d'ordinateurs, surveillent, épient toutes les activités physiques et intellectuelles et utilisent cette information, pas toujours avec subtilité, pour manipuler et exploiter leurs semblables.

Le trait commun de tous ces récits est le lien qu'ils établissent entre ordinateur et pouvoir. C'est d'ailleurs la peur de cet élément nouveau dans la structure classique du pouvoir qui constitue la principale source d'inquiétude au sujet de la vie privée. L'avènement de l'ordinateur provoque à notre époque une révolution qui n'est pas sans analogie avec celle qu'a entraînée la découverte du fer dans les temps préhistoriques. Comme les armes façonnées du nouveau métal ont dû constituer un élément clé dans les anciennes structures du pouvoir, ainsi en est-il aujourd'hui de l'ordinateur

qui est capable de stocker, manipuler et transmettre les données. Selon certains auteurs, la vie privée dans son rapport à l'information soulève une question politique plutôt que juridique. Si les organismes et établissements possèdent de plus en plus de renseignements sur les individus, le flot d'information en sens inverse est peu considérable.

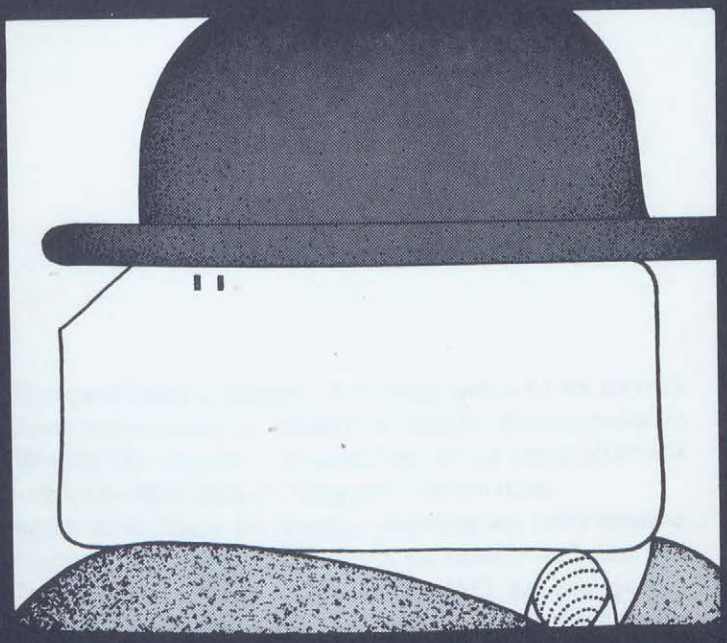
Cependant, l'ordinateur, outil de centralisation aussi bien que de diffusion, pourrait désormais servir à une nouvelle répartition de l'information (et en ce sens, du pouvoir) entre les administrations et les individus. Car s'il est impossible à une personne de tenir plus d'une conversation à la fois, l'ordinateur peut non seulement transmettre simultanément à de nombreux interlocuteurs une masse d'information, mais il est capable de recevoir en même temps leurs points de vue sur une variété de sujets. Il est également capable de limiter l'accès de dossiers ou de parties de dossiers aux personnes autorisées. En outre, l'automatisation des fichiers conduisant normalement à la centralisation, il devient plus facile de contrôler l'accès à l'information personnelle – plus facile, aussi, d'abuser des possibilités qui s'offrent de centraliser le contrôle.

Si telle est la volonté politique, l'ordinateur peut très efficacement contribuer à la diffusion de l'information et par conséquent, dans la mesure où les deux se tiennent, au partage du pouvoir. Comme tout instrument puissant, l'ordinateur peut servir le bien comme le mal, et il ne cessera d'inspirer la terreur qu'après avoir été clairement affecté au seul service du bien. Son influence, jusqu'ici, semble avoir été très bénéfique en matière de productivité et de gestion, mais la question de ses répercussions sociales est loin d'être réglée.

[1] SCHWARTZ, Barry, « The Social Psychology of Privacy », *American Journal of Psychology*, mai 1968, p. 752

[2] HARRINGTON, Michael, cité par MILLER, Arthur, dans « The Assault on Privacy », Ann Harbour : University of Michigan Press, 1971, p. 258.

Deuxième partie



Résultats d'enquêtes

Introduction

Le Groupe d'étude a consacré une bonne partie de ses travaux aux pratiques canadiennes en matière de collecte, de manipulation et de diffusion de données personnelles, et au comportement professionnel des exploitants de banques d'information.

Étant donné la masse des données personnelles, notre enquête a nécessairement été fragmentaire et n'a pu aboutir qu'à une vue incomplète et momentanée de la situation en 1971. Les pratiques et les opinions changent rapidement; aussi faut-il se garder des extrapolations imprudentes. Néanmoins nous estimons qu'une information partielle peut être profitable si on y recourt avec circonspection. Un aperçu, tout imprécis qu'il soit, peut être d'un précieux concours dans la découverte des voies à suivre.

La partie consacrée à la collecte des données comprend six chapitres. Dans le deuxième, nous exposons les méthodes de collecte et formulons quelques observations générales, mais la diversité des conditions et des pratiques en limite la portée. Les quatre chapitres suivants sont consacrés au traitement de l'information sous les rubriques ci-après : données statistiques, données administratives (y compris les données financières et médicales) et données d'enquête ou d'investigation. Cette répartition n'embrassant pas tous les cas, nous nous sommes permis certaines libertés dans le classement des organisations. Enfin, dans le dernier

chapitre, nous traitons succinctement la question du numéro d'identification unique.

Nous n'avons pas tendu vers une approche rigoureusement objective, mais nous nous sommes prononcés chaque fois que les pratiques de manipulations des données le justifiaient. Les banques d'information étrangères ont retenu notre attention sous la rubrique « compagnies de crédit et d'assurance » et non comme catégorie homogène – ce qui eût été erroné. D'autre part, certains aspects de ces problèmes ont été exposés plus longuement s'ils nous semblaient d'intérêt général – car il ne s'agissait pas de faire un exposé fidèle et équilibré des usages en cours dans l'exploitation des banques d'information. Ainsi, nous avons consacré une section du chapitre 3 au problème de la divulgation non intentionnelle de données statistiques.

Sauf indication contraire, la matière de la présente partie a été tirée de l'étude effectuée pour notre Groupe par le professeur J. Carroll, et intitulée : *Personal Records : Procedures, Practices and Problems*.

Chapitre 2
Les systèmes d'information

1. Nos sources

Pour recueillir l'information dont il avait besoin, le Groupe d'étude a eu recours à diverses méthodes.

a. Le questionnaire

Les données de base touchant la manipulation de l'information sur les personnes proviennent des réponses à un questionnaire (voir appendice) adressé à 2 516 organisations canadiennes qui étaient censées tenir d'importants fichiers d'information personnelle. Pour en établir la liste, nous avons consulté les répertoires des principales entreprises financières et industrielles du Canada, des associations œuvrant en divers domaines (enseignement, assistance sociale, assurance, santé et syndicalisme), et celui des utilisateurs d'ordinateurs établi par l'Association canadienne d'informatique. Nous nous sommes adressés non seulement à des organisations utilisatrices d'ordinateurs, mais à des organisations dotées de fichiers manuels.

L'élaboration de notre questionnaire s'est effectuée en consultation avec le professeur Westin qui commençait alors à recevoir

des réponses à celui qu'il avait établi pour l'Académie nationale des sciences des États-Unis. Les renseignements recherchés par notre enquête se répartissent entre trois grandes catégories :

- données de base sur les activités de l'organisation, la taille et la composition de ses fichiers et caractéristiques de son matériel informatique ;
- renseignements sur la manipulation de l'information personnelle et sur les politiques, explicites ou non, en la matière ;
- renseignements sur les attitudes à l'égard, notamment, d'une réglementation et d'un code déontologique éventuels ; sur les diverses conceptions quant à l'établissement de mesures de sécurité.

Le taux de réponse a été de quelque 50 p. 100 (1 268). De plus, près de 200 organisations nous ont écrit pour nous expliquer leur abstention. La plupart invoquaient le manque d'informations et de temps. Celles qui n'ont pas répondu étaient surtout de petites entreprises ou des associations régionales. Parmi les exploitants de grands systèmes d'information, moins de 100 se sont abstenus. Quant aux organisations qui ont rempli le questionnaire, elles employaient à peu près 1,2 million de personnes au total, soit le sixième de la population active du Canada. Près de la moitié des réponses venaient du secteur public, c'est-à-dire d'organismes fédéraux, provinciaux ou municipaux. Pour la répartition des réponses selon les domaines, voir le tableau 1.

Les questions avaient été groupées sous différentes rubriques, correspondant chacune à un type de fichier (employés, crédit, etc.) ; et le tableau ci-après indique les pourcentages pour chaque rubrique.

Employés	25,4 p. 100
Crédit	20,8 p. 100
Santé	14,7 p. 100
Services sociaux	7,4 p. 100
Éducation	6,0 p. 100
Assurance	6,0 p. 100
Corps policiers	1,7 p. 100
Divers	18,0 p. 100
	100 p. 100

D'une manière générale, les organisations disposant de grandes quantités d'information personnelle étaient bien représentées. Toutefois, l'interprétation des résultats exige une extrême prudence, car l'échantillonnage était très disparate. La diversité des

Tableau 1

Ventilation des réponses suivant la vocation des organisations*

	Réponses	Pas de réponse	Diffusion du questionnaire
Banques, établissements de crédit et institutions assimilées	61	49	110
Assurance-vie, assurance-accidents assurance-sinistres	76	41	117
Services publics	38	6	44
Media	8	17	25
Santé ou statistiques démographiques	182	183	365
Éducation	76	45	121
Fiscalité	2	14	16
Permis de conduire ou immatriculation des véhicules	2	0	2
Commerce	22	21	43
Cartes de crédit voyage-distraction	1	1	2
Compagnies pétrolières	22	7	29
Sociétés de placement	64	120	184
Police, mise en liberté surveillée, libération sur parole	11	4	15
Assistance sociale	39	8	47
Enregistrement des hypothèques sur les biens meubles	1	0	1
Échange d'information sur le crédit	10	16	26
Secteur des services	83	111	194
Grands employeurs industriels	127	84	211
Organismes de réglementation	7	9	16
Bureaux de placement	11	27	38
Études des marchés	1	0	1
Associations (ouvrières, professionnelles)	95	337	432
Œuvres de charité	54	50	104
Fournisseurs de répertoires d'adresses	2	4	6
Enquêteurs privés, agents de recouvrement, experts en sinistres	43	68	111
Divers	198	0	198
Question sans réponse	36	0	36
TOTAUX	1272	1222	2494

*Le libellé de la question est tel qu'il suit:

« Comment caractérisez-vous la fonction primordiale de votre organisme? (Marquez *une* seule catégorie). »

Dans la plupart des catégories, on a obtenu plus de 50 p. 100 de réponses sauf dans celle des « associations » où nombre d'organisations régionales et de conseils locaux de syndicats ouvriers n'ont pas rempli le questionnaire quand leur association nationale l'avait fait ou avait soumis un mémoire. En outre, il semble que diverses administrations publiques (fiscalité), notamment des municipalités, se soient classées dans la catégorie « divers ».

intérêts et des vocations était extrême et de plus le poids statistique affecté aux réponses d'un grand service provincial de santé, par exemple, était le même que pour une entreprise n'employant que 20 personnes. En conséquence, les données ont plus de signification considérées par groupes fonctionnels et rapprochées d'autres informations recueillies par le Groupe d'étude.

b. Entrevues

Nous avons tenu à vérifier la validité des réponses au questionnaire et à familiariser les membres du Groupe d'étude avec les problèmes quotidiens des exploitants de banque d'information; à cette fin, des entrevues ont été ménagées dans 43 établissements de toutes dimensions, choisis de façon à assurer la meilleure représentation possible des régions et des secteurs d'activité. Chaque établissement a reçu la visite d'une équipe de deux à quatre enquêteurs, dont un juriste et un informaticien.

Ces enquêtes sur place ont permis de recueillir des renseignements précieux sur les problèmes d'exploitation et sur les méthodes en usage. À ce propos, le Groupe d'étude tient à remercier tous ceux qui ont accepté de recevoir ses membres.

c. Mémoires

Une communication a été adressée à 187 associations. Le Groupe d'étude y invitait les associations à faire connaître leurs vues dans un mémoire ou à solliciter celles de leurs membres. Ne voulant pas limiter son enquête à un petit nombre d'associations qui avaient déjà manifesté leur intérêt, le Groupe d'étude optait pour une notification aussi massive, quitte à recevoir peu de réponses. De fait, seize mémoires seulement lui ont été présentés, mais ils contenaient des renseignements d'une valeur inestimable.

Nous avons eu accès en outre aux mémoires du Groupe d'étude sur la téléinformatique au Canada avec lequel nous entretenions une étroite relation. Sur ses 200 mémoires, 54 faisaient valoir la nécessité de mesures pour protéger l'information personnelle, dont 22 contenant des observations précises ou des recommandations.

d. Sources diverses

Le Groupe d'étude a eu recours aussi à des sources complémentaires, dont les suivantes : réponses de treize sociétés américaines tenant des fichiers d'information personnelle sur des Canadiens et auprès desquelles on avait cherché à se renseigner sur les pratiques en matière de manipulation de l'information personnelle (voir la liste de ces sociétés en appendice) ; rapport d'une enquête sur les attitudes face à l'ordinateur, menée par le *Social Survey Research Centre* pour le ministère des Communications ; diverses études indirectement reliées aux travaux du Groupe d'étude.

2. Systèmes d'information et données personnelles

a. Résumé des résultats

Souvent les informations recueillies n'avaient de signification que par rapport à des groupements particuliers ; elles accusaient des disparités de comportements et des divergences d'intérêt. Il a tout de même été possible de tirer certaines conclusions générales sur la manière dont est traitée l'information personnelle.

1) Les échanges d'information sont plus nombreux qu'on ne le pense généralement dans le public. Un réseau se crée dès que l'échange présente de l'intérêt pour deux détenteurs d'information personnelle. Étant donné le caractère non organique de ces échanges, on ne saurait définir avec exactitude leurs cheminements. Toutefois les réponses au questionnaire ont fourni quelques renseignements sur les réseaux. Les corps policiers, les agences de renseignements commerciaux, les compagnies d'assurance, les autorités de l'enseignement et les services d'assistance sociale pratiquent tous, sur une échelle plus ou moins grande, ce genre d'échanges, qui généralement s'effectuent à l'insu des personnes en cause. De nombreuses organisations, surtout parmi les plus importantes, ont défini des règles de sécurité limitant l'accès aux fichiers d'information personnelle ; il ne semble pas, toutefois, d'après quantité de témoignages par des tiers, que ces règles soient appliquées

dans les communications faisant intervenir des personnes connues pour leur discrétion.

2) La collecte et l'utilisation de l'information personnelle par les gouvernements semblent inquiéter davantage. D'ailleurs, il est très significatif que de hauts fonctionnaires aient souvent exprimé de l'inquiétude à propos des systèmes d'information gouvernementaux.
Dans son mémoire au Groupe d'étude sur la téléinformatique, le *Newfoundland and Labrador Computer Service Centre* , qui est un organisme provincial, écrivait ce qui suit : « Les gouvernements, qui sont les plus exposés à l'abus de l'information qu'ils recueillent sur les citoyens... devraient élaborer des politiques propres à prévenir ce mal. »
Le ministère fédéral de la Main-d'œuvre et de l'Immigration faisait ressortir, dans son rapport, un trait particulier des banques d'information personnelle : « On sera amené naturellement, par souci d'efficacité, à intégrer les banques d'information à des banques analogues des autres ministères, des gouvernements provinciaux, des services municipaux d'assistance sociale, voire aux banques d'organismes privés. Il en résultera une amélioration considérable des services sociaux. Mais nous pourrions aussi être les témoins de l'érosion progressive de la vie privée ... il serait donc souhaitable que soient établies des règles touchant le regroupement des banques d'information. » Des opinions semblables ont été exprimées par le gouvernement du Nouveau-Brunswick, ainsi que par plusieurs ministères fédéraux.

3) On a noté très peu de différence dans la manière de manipuler l'information entre les organisations publiques et les organisations privées. Toutefois, groupées par domaines d'activité (crédit, médecine, recherche, enquête), elles accusaient des dissemblances considérables.

4) Le rôle de l'ordinateur dans le traitement de l'information strictement personnelle a été restreint jusqu'ici, mais il gagne en importance. Actuellement, un fichier type géré par ordinateur comporte de 1 000 à 5 000 articles de 300 caractères chacun, et qui font l'objet d'un traitement 10 à 20 fois par an. Les coûts

d'utilisation de l'ordinateur diminuant, la gestion automatisée de petits fichiers, peu consultés, deviendra de plus en plus pratique. D'autre part, en raison de l'augmentation des appointements et des salaires et de la complexité croissante de nos structures économiques et sociales, sans doute verra-t-on se multiplier au sein d'organisations de nature et de taille variées les systèmes de gestion automatisés[1].

5) Les erreurs dans les systèmes de gestion de l'information personnelle sont plus nombreuses qu'on ne croit généralement. Ainsi, 75 p. 100 des personnes interrogées signalaient qu'elles avaient découvert des erreurs dans les fichiers à l'occasion de leur automatisation. Aux États-Unis, dans un secteur d'activité où l'on s'attendrait à plus de rigueur, la conversion d'un fichier manuel de la police a permis de constater des erreurs dans près du tiers des dossiers. Comme on procède souvent à des échanges de données, une erreur dans un fichier risque de se répercuter dans plusieurs autres.

6) La plupart des systèmes d'information ont, en un certain sens, un caractère local, mais grâce aux échanges d'information ils pourraient fonctionner à une échelle nationale ou internationale. Cependant les organisations d'envergure nationale ou internationale passent vite à un système d'information adapté à leur rayonnement géographique.

7) D'après les résultats d'une enquête effectuée pour le ministère des Communications[2], plus d'un tiers des Canadiens estiment que les ordinateurs représentent une menace pour leur vie privée, et plus de la moitié estiment que les ordinateurs entraîneront la violation du caractère confidentiel des informations personnelles. L'imprécision des termes « vie privée » et « caractère confidentiel » (qui n'avaient pas été définis pour les fins de l'enquête) n'a pas manqué de créer une certaine confusion; l'inquiétude générale est significative toutefois.

8) Les exploitants de banques d'information, plus particulièrement de grandes banques d'information personnelle, ont presque tous accepté le principe d'une réglementation dans ce domaine, montrant

ainsi combien ils sont sensibles au problème de la protection de l'information personnelle.

Pour être général, cet accord n'en masquait pas moins de grandes divergences de vues. Plusieurs organisations, tels le *Canadian Book Publishers' Council* et l'Association des banquiers canadiens, estiment que « le droit à l'information » est plus important que les vagues allégations de violations de la vie privée. D'autres, dont l'Association des manufacturiers canadiens et la *Retail Credit Company of Canada*, estiment inutile ou prématurée toute législation à cet égard.

Les systèmes canadiens d'information se prêtent à d'autres observations de caractère général.

b. Degré d'automatisation

La décision d'utiliser un ordinateur pour le stockage des informations personnelles tient à divers facteurs, dont le développement technique de l'entreprise, sa situation financière, sa politique de gestion, la fréquence des consultations et des mises à jour de ses fichiers, le nombre et la structure des dossiers actifs.

Tous ces facteurs peuvent se modifier; en fait, ce sont surtout les caractéristiques d'un fichier (taille, structure et utilisation) qui déterminent si l'automatisation est opportune. À titre d'exemple, un fichier de 10 000 unités, dont 10 p. 100 consultées ou mises à jour chaque semaine, pourrait utilement être automatisé. La taille et le degré d'utilisation interviendront tour à tour comme facteur prédominant. Il peut s'avérer également rentable d'automatiser un petit fichier à taux de consultation élevé ou un grand fichier rarement consulté.

La moitié des enquêtés ont recours au traitement électronique de l'information; parmi eux, les deux tiers auraient leurs propres ordinateurs; les autres s'adressent à des façonniers. La moitié des utilisateurs sont venus à la mécanographie entre 1965 et 1969. Par la suite, le nombre des organisations à se convertir à l'informatique a décru nettement; l'étape de maturité aurait donc été atteinte. Il semble aussi qu'on se préoccupe assez généralement d'améliorer les systèmes en usage, car les installations nouvelles sont moins nombreuses. D'ailleurs, dans l'enquête du Groupe d'étude sur la téléinformatique au Canada, le taux de croissance cumulée de cette branche était établi à 17 p. 100 pour la décennie 1970-1980.

Plus de la moitié des enquêtés qui ont automatisé leurs fichiers

estiment l'ordinateur avantageux mais non indispensable; 10 p. 100 sont d'avis qu'il n'a guère changé les choses. Seulement 40 p. 100 le considèrent comme nécessaire à la poursuite de leurs activités.

Dans nombre de cas les fichiers automatiques complètent le classement traditionnel. Ainsi 90 p. 100 des utilisateurs de fichiers automatisés consignent des informations sur les mêmes personnes dans des fichiers manuels. Les trois quarts de ces organisations conservent l'information la plus confidentielle et délicate dans des dossiers. Manifestement le problème de la protection de l'information personnelle déborde celui de l'ordinateur.

Parmi les organisations dotées de systèmes informatiques, 32 p. 100 estiment être en mesure de grouper leurs informations concernant chaque personne sur une seule fiche, et 16 p. 100 que l'automatisation des fichiers a rendu plus facilement identifiables les données transmises à l'État. Un peu moins de 40 p. 100 estiment que l'ordinateur a accru le volume des informations sur chaque personne; les autres ont noté peu de changement. Seulement 3 p. 100 font observer que l'automatisation a entraîné la création de nouveaux règlements sur l'accès aux dossiers par les personnes en faisant l'objet.

c. Normes et pratiques en matière de sécurité

Souvent on confond sécurité et vie privée. La première, en ce qui nous concerne, est liée aux mesures qui tendent à assurer la protection de l'information personnelle; la seconde correspond à une notion juridique et sociologique relativement complexe (voir le chapitre premier). Lorsqu'il faut restreindre l'accès à l'information personnelle, il va de soi que des mesures de sécurité s'imposent. Il y a donc lieu de tenir compte des mesures de sécurité et des attitudes à cet égard, dans une étude pratique sur la vie privée face à l'information. Les raisons qui poussent les organisations à protéger leurs informations sont souvent sans rapport avec la défense de la vie privée. Une organisation, par exemple, voudra préserver le secret de certaines opérations commerciales ou protéger ses installations informatiques contre le vandalisme et le sabotage.

Les données statistiques touchant les mesures de sécurité en vigueur au Canada sont peu significatives par référence à l'ensemble des systèmes d'information. Certains chiffres cependant permettent de dégager une vue d'ensemble. Parmi les enquêtés, 23 p. 100 n'estiment pas qu'il y ait lieu d'exercer des contrôles pour prévenir les utilisations indues de l'information par le personnel.

Parmi ceux qui ont recours à une surveillance, le huitième ont pris des employés en défaut et les ont poursuivis ou sanctionnés. Les organisations à fins non lucratives formaient la majorité dans cette catégorie. Les trois quarts des enquêtés disposant d'ordinateurs surveillent l'accès du matériel et 40 p. 100 appliquent des mesures de sécurité (mots de passe, identification par code et chiffrement). La même proportion des entreprises soumettent le personnel informatique à des vérifications de probité et plus des deux tiers ont recours à des méthodes efficaces pour la destruction des bandes et des imprimés devenus inutiles.

La question : « Quelle est votre ligne de conduite en cas de divulgation d'informations sur un sujet identifié ? » a suscité diverses réponses. Le tiers appliquent des consignes écrites, 55 p. 100 des consignes verbales, et les autres n'ont pas de ligne de conduite définie. Les grandes organisations utilisant un matériel perfectionné attachent généralement plus d'importance que les autres à la sécurité. Les clients ont deux fois et demie plus de chances que les employés d'être protégés par des dispositions écrites, mais ces derniers bénéficient de consignes verbales dans 70 p. 100 des organisations et d'une simple politique de non-divulgation dans 14 p. 100.

d. L'échange d'information

L'analyse des réponses à certaines questions permet de reconstituer le cheminement des données entre des organisations à vocation différente. On constate que les réseaux de liaisons s'établissent selon un schéma cohérent et qu'ils sont beaucoup plus développés que ne l'imaginent ceux qui n'ont pas étudié cette question. Un agent d'assurance de Colombie-Britannique, par exemple, signalait combien il est facile d'obtenir des renseignements sur les personnes, leur situation financière et leur conduite, quand on est connu dans un certain réseau d'échange d'information; par ailleurs, d'après une enquête sur le « droit à la vie privée »[3], effectuée en Angleterre, certaines agences offrent des informations sur le détail des comptes bancaires personnels pour $ 15,75, et il est possible d'obtenir des numéros de téléphone ne figurant pas dans l'annuaire pour un peu plus de $ 10.

Le recours à des enquêteurs pour des renseignements personnels est particulièrement fréquent parmi les corps de police et les compagnies d'assurances. Les services d'assistance sociale, les organismes de réglementation, les entreprises commerciales et les grandes entreprises industrielles, selon l'ordre d'importance sous ce

rapport, s'adressent aussi aux agences de renseignements commerciaux et aux enquêteurs privés. Mais les centres médicaux et les établissements d'enseignement sont aussi très souvent consultés ; ils sont en effet des sources d'information personnelle au même titre que les employeurs.

La plupart des systèmes d'information présentent un caractère local, mais, grâce à des accords d'échanges, ils ont la possibilité de mener des opérations d'envergure nationale ou internationale. Parmi les enquêtés, 48 p. 100 fournissent des informations personnelles à des correspondants aux États-Unis. Cette catégorie comprend surtout agences de renseignements commerciaux, organismes de réglementation, corps de police, grandes industries, compagnies d'assurances, entreprises commerciales et bureaux de placement. Les fournisseurs de répertoires d'adresses et les bureaux des véhicules automobiles communiquent aussi des données à des correspondants américains. Parmi les enquêtés, 59 p. 100 recevraient des informations personnelles de correspondants américains.

e. Mise à jour des fichiers

Plus de la moitié des enquêtés conservent des informations sur les employés plus de sept ans après leur départ. Seulement 15 p. 100 écartent les articles non mouvementés dans les 18 mois ; les deux tiers d'entre eux procèdent à leur destruction, et le tiers transfèrent ces informations aux archives ; quatre organisations (moins de 0,5 p. 100 des enquêtés) renvoient les dossiers aux intéressés.

f. Localisation des fichiers

D'après les réponses au questionnaire, cinq organisations seulement, dont quatre syndicats, ont tous leurs fichiers aux États-Unis. De plus, 66 p. 100 des enquêtés ont leurs fichiers d'information personnelle dans la province même où ils exercent leur activité. Mais 26 p. 100 des enquêtés les centralisent dans une autre province du Canada ; 8 p. 100 conservent aux États-Unis, en totalité ou en partie, l'information personnelle. Cette catégorie comprend, outre les syndicats, des sociétés pétrolières, des compagnies d'assurances, des services de santé et des établissements de prêt. Parmi les organisations qui conservent une partie de leur information aux États-Unis, près de la moitié ont été constituées ailleurs qu'au Canada.

D'autre part, 76 p. 100 des enquêtés prévoient ne jamais avoir

de fichiers aux États-Unis. Les autres, s'ils ne l'ont déjà fait, en établiraient volontiers dans ce pays, s'ils y voyaient quelque avantage.

g. Les plaintes

Dans le questionnaire, on demandait aux organisations si elles avaient reçu des plaintes – de personnes ou de groupes représentant les intérêts de ces personnes – à propos de la divulgation d'information personnelle à l'extérieur. Les trois quarts des enquêtés ont donné une réponse négative et 15 p. 100 ne pouvaient répondre ou trouvaient la question inappropriée. Parmi ceux qui ont répondu affirmativement, 10 p. 100 (soit 121) en reçoivent à l'occasion. Quatre organisations seulement reconnaissent la fréquence des plaintes. S'il est difficile de fonder des statistiques sur un échantillon aussi limité, il convient de noter que deux des organisations étaient des hôpitaux, et les deux autres, des agences d'enquête.

Les plaintes relatives aux méthodes de collecte accusent à peu près la même répartition proportionnelle que celles touchant la divulgation. Cinq organisations seulement reconnaissent faire l'objet de plaintes fréquentes, dont trois œuvrant dans l'assurance ou l'expertise des sinistres.

Pour 16 p. 100 des enquêtés, les individus (ou les groupes représentant leurs intérêts) cherchent occasionnellement à consulter leurs dossiers ou bien formulent des plaintes sur la ligne de conduite de l'entreprise en la matière. Moins de 1 p. 100 (pour la plupart, des hôpitaux) reçoivent fréquemment ce genre de demande. Pour les autres, la chose ne se produit jamais, ou du moins pas qu'ils sachent.

Parmi les organisations qui ont automatisé la gestion de leurs fichiers personnels, les trois quarts ont admis que la conversion leur a permis de déceler et de corriger des erreurs. Ces erreurs étaient très graves pour 13 p. 100 d'entre eux et de peu d'importance pour 30 p. 100. Ce résultat permet d'apprécier le degré d'exactitude des informations contenues dans la plupart des fichiers.

À ce sujet, on peut citer l'expérience d'une compagnie d'assurance-vie canadienne qui, il y a quelques années, mettait sur bandes magnétiques les données de centaines de milliers de polices d'un fichier à cartes perforées. On s'est alors aperçu que le fichier comportait en moyenne une erreur par police. Il a donc fallu vérifier et corriger les informations, et différer le programme de conversion de deux ans. On a déjà signalé qu'aux États-Unis

l'automatisation des fichiers de la police a révélé qu'une information sur trois était erronée.

Lors de l'enquête sur les attitudes des Canadiens face à l'ordinateur, menée par le *Social Survey Research Centre* pour le ministère des Communications, 30 p. 100 des personnes interrogées déclaraient qu'elles-mêmes ou des proches avaient constaté dans leurs factures, leurs souscriptions ou leur compte de crédit, des erreurs attribuables à l'ordinateur.

h. Les attitudes et points de vue

Évidemment, les réponses des porte-parole aux questions touchant le respect de l'information personnelle varient beaucoup suivant le domaine d'activité de l'organisation dont ils font partie. L'agent de police, qui voit sans cesse des délinquants exploiter les subtilités de la loi pour éviter l'arrestation ou la condamnation, se souciera moins du respect de l'information personnelle que Statistique Canada, organisme pour lequel il ne s'agit pas là d'une simple obligation de droit, mais bien d'un impératif absolu, s'il ne veut pas tarir les sources d'information dignes de foi.

Le questionnaire proposait une série de mesures propres à assurer la protection de l'information personnelle et demandait aux organisations d'indiquer leur attitude en choisissant parmi les cinq ci-après : vive approbation, approbation, neutralité, opposition, vive opposition. À la figure 1, on trouvera la ventilation des réponses. Lorsqu'un groupe d'organisations s'est singularisé par sa position, il en est fait état dans la colonne « réaction ».

Quatre propositions ont fait l'accord général, échappant même à toute opposition sensible d'un groupe particulier. Ce sont les suivantes :

- il faudrait que toute personne faisant l'objet d'un dossier contenant des informations propres à l'individualiser ait le droit de les corriger, rejeter et mettre à jour et de les épurer des données inexactes ou périmées, le cas échéant ;
- il faudrait que des normes de sécurité soient obligatoires pour les banques de données personnelles ;
- il faudrait adopter des normes pour la collecte et la diffusion des informations ;
- l'information périmée devrait être périodiquement éliminée des fichiers.

L'idée que fournisseurs, banques d'information et courtiers en données soient assujettis à l'obligation de la licence a fait l'objet

d'un accord presque général. Seul le groupe des propriétaires de media (sept réponses en tout) a marqué une vive opposition. Peut-être craignait-il pour la liberté de la presse.

L'idée de l'enregistrement des banques d'information quant à leur fin et à leur contenu a suscité une réaction analogue.

Les réactions au principe voulant que l'individu sur lequel on ouvre un dossier en soit averti ont été très favorables, mais les agences de renseignements commerciaux ont manifesté leur vive opposition pour des raisons que nous verrons au chapitre 4.

Le droit de prendre connaissance sur demande de son propre dossier est plus discuté. Les corps de police, les organismes de réglementation, les compagnies d'assurance et les services de santé désapprouvent cette proposition. Apparemment, il y aurait contradiction entre ce résultat et l'approbation presque unanime du droit pour les individus de corriger, rejeter ou mettre à jour les informations portées à leur dossier. On peut croire que les groupes opposés au droit pour chacun de voir son dossier n'ont pas envisagé toutes les conséquences de celui de rectifier l'information au besoin.

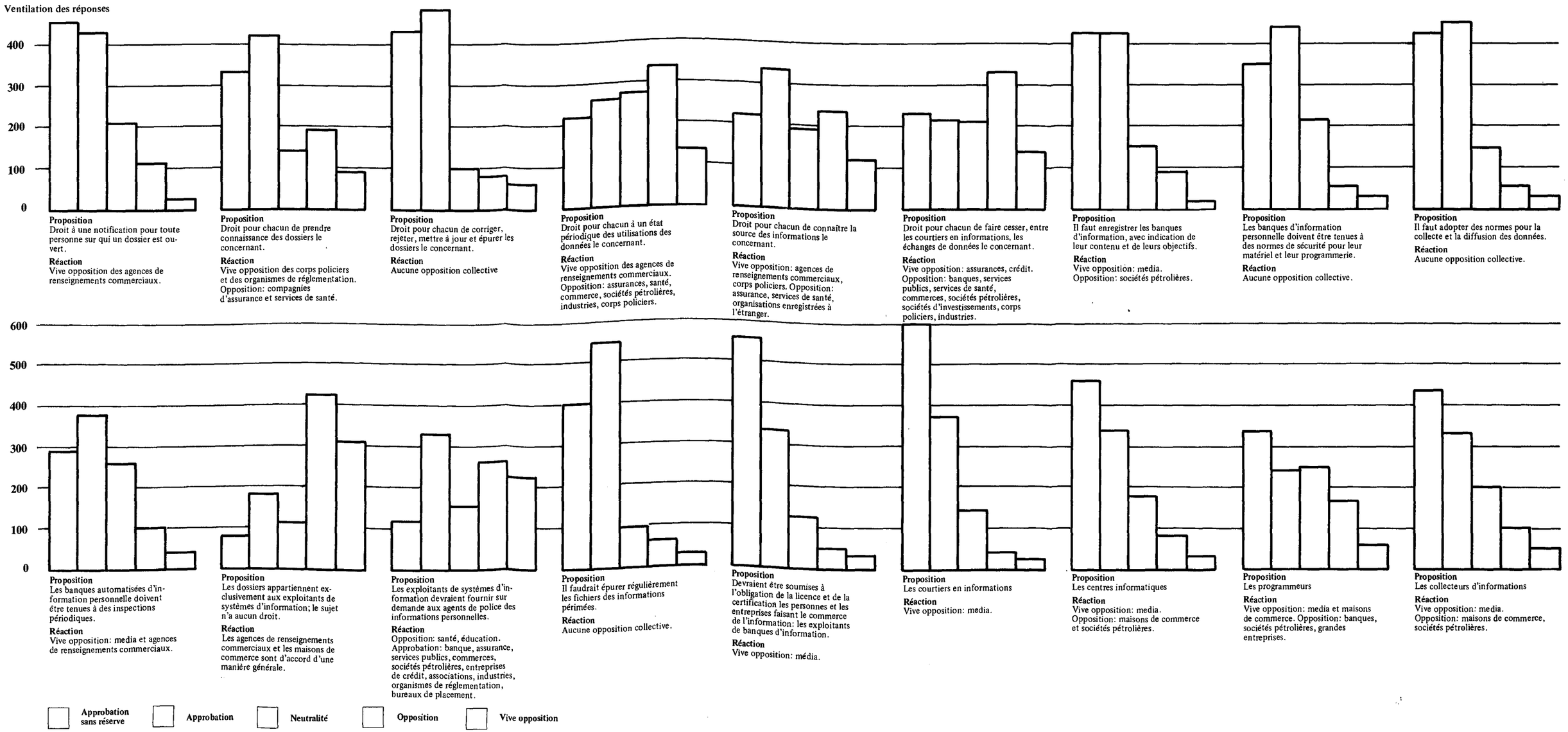
Les réponses aux trois propositions suivantes ont été très partagées :

- droit pour l'individu à un état périodique des utilisations de l'information le concernant ;
- droit pour l'individu de connaître l'origine des informations se trouvant dans son dossier ;
- droit pour l'individu de faire cesser tout échange de renseignements le concernant entre les courtiers en informations.

Il n'y a pas eu accord non plus quant à la question de savoir si les banques d'information devraient, sur demande, fournir des renseignements personnels aux corps de police. On a rejeté aussi l'idée selon laquelle l'information personnelle consignée dans les fichiers serait considérée comme propriété exclusive des banques d'information, sans que les individus en cause aient droit de regard sur cette information. Toutefois les agences de renseignements commerciaux, les entreprises commerciales et un certain nombre d'autres organisations y ont souscrit.

Figure 1

Attitudes selon les réponses au questionnaire



3. Classification des banques d'information

À la lumière de notre étude, nous croyons utile de répartir les banques d'information entre trois grands domaines : statistique, administration et renseignements.

Banques d'information statistique

- Les données traitées ne se présentent qu'en résultats globaux. Les personnes ne sont ni ne doivent être identifiables.
- Les données en entrée sont souvent de nature à identifier l'individu ; elles sont souvent stockées sous cette forme de façon que l'agrégation comporte un grand nombre de variables distinctes.
- Les données appartiennent à toutes ou presque toutes les catégories d'information que l'on peut considérer comme personnelles.
- Les banques d'information sont considérables pour bon nombre ; généralement elles se prêtent bien à l'emploi d'ordinateurs pour le tri et la réduction des données.
- Indépendamment des exigences de la loi, les organismes de statistiques, tel Statistique Canada, ont tout intérêt à préserver le caractère confidentiel des données. En effet, pour continuer de recueillir des données exactes, ils ont besoin de la confiance qu'on leur accorde ; c'est pourquoi certains, dont Statistique Canada, sont tenus de protéger le caractère confidentiel des données.

Les banques d'information administrative

Les entreprises ne peuvent se passer d'information administrative. L'information recueillie peut varier en volume, ainsi que par ses fins et son caractère plus ou moins confidentiel.

- En règle générale, l'aspect sécurité ne prime pas et la protection de l'information personnelle n'est pas une préoccupation essentielle. Seuls les abus patents donnent lieu à des mesures.
- Dans nombre de cas (assistance sociale, enseignement et placement), il y a relation de dépendance entre

l'administrateur et l'administré ; celui-ci ne peut guère contribuer à la décision sur le type d'information à fournir et sur son exploitation ultérieure.

- Dans un service donné, l'information administrative ne présente un caractère névralgique que dans un ou deux domaines à la fois ; ainsi des informations médicales et des informations sur le revenu ne coexistent généralement pas dans un même fichier (sauf dans le cas particulier où une personne réclame un abattement d'impôt pour des frais médicaux).
- Comme les banques d'information administrative ont souvent des intérêts parallèles (la situation financière des clients, par exemple), il arrive que des pressions les contraignent à effectuer des échanges. On effectue parfois ceux-ci dans les formes pour réduire les frais, notamment quand ces échanges se font au sein d'une même organisation (entre services gouvernementaux ou conglomérats, par exemple).
- Les individus peuvent retirer des avantages appréciables de l'existence de ces fichiers (permis de conduire, prestations sociales, emploi, etc.) ou de la diffusion des renseignements qu'ils contiennent (prêts consentis en raison de l'information fournie par l'employeur, information médicale communiquée à l'occasion d'une urgence, etc.).

Les banques de renseignements

- S'il existait une confiance entière entre tous les membres de la société, on n'aurait jamais songé à créer des banques de renseignements. Le service de renseignements de la police illustre bien cette assertion, mais les agences de renseignements commerciaux et les enquêteurs privés, qui rassemblent des renseignements pour les employeurs et les compagnies d'assurances essentiellement, ont la même raison d'être.
- Les renseignements consignés dans les dossiers sont souvent très complets (données médicales, sociales, financières, judiciaires, etc.).
- Les sources d'information sont le plus souvent le ouï-dire.
- Des personnes qui font l'objet d'un dossier (et d'une enquête) n'en savent généralement rien.

[1] Dans ses grandes lignes, le système de gestion automatisée est un ensemble de moyens mis en œuvre pour traiter et présenter les données de sorte que les cadres de la gestion disposent de l'information nécessaire à l'exécution de leurs tâches. On a souvent mis en doute l'efficacité de ces systèmes, notamment leur utilité pour les cadres supérieurs chargés principalement de la planification stratégique. Il apparaît néanmoins qu'ils comporteront des atteintes à la vie privée à un palier inférieur de la gestion. Les possibilités actuelles sont nettement suffisantes à ces niveaux.

[2] Étude sur les attitudes du public à l'égard de l'ordinateur. Elle a été effectuée indépendamment des travaux du Groupe d'étude par le Social Survey Research Centre, de Toronto, pour le ministère des Communications. Son rapport sera publié au cours de l'année.

[3] « Report on the Right of Privacy », étude de l'Oxford Group of Labour Lawyers, mars 1971.

Chapitre 3
Les statisticiens

La lutte pour l'amélioration de notre niveau de vie et les progrès réalisés en ce sens ont fait naître, dans les secteurs public et privé, une avidité insatiable de statistiques économiques. Il ne s'agit pas d'une curiosité malsaine, mais d'un effort pour maîtriser les paramètres déterminant la vie de notre société, dont la complexité tiendrait, en partie du moins, à notre souci d'efficacité. Aussi, la société s'est-elle largement transformée en un univers de spécialistes. Puis la spécialisation a entraîné la diversification dans les structures du pouvoir, ce que Drucker appelle « nouveau pluralisme », dans *The Age of Discontinuity*[1]. La complexité même du système économique où nous vivons exige que la raison et l'intuition soient guidées dans leurs démarches par des données statistiques. Cette règle s'applique aux gouvernements, qui doivent décider de l'opportunité de nouvelles politiques et distinguer la portée des anciennes, et aux entreprises qui, pour rester compétitives, doivent se tenir au courant des besoins du marché.

En constatant que sont dépassés les anciens critères économiques sur lesquels reposaient les décisions, on a suscité une demande accrue d'informations de nature extrêmement variée. Dans les universités, la faveur de l'économie et de la physique nucléaire a cédé à celle de la sociologie et de l'informatique ; la conjonction de

celle-ci et des disciplines connexes a donné naissance à d'innombrables études « quantitatives » tendant à mettre de l'ordre dans nos connaissances des desseins, des attitudes et du comportement de l'homme.

La floraison de la recherche dans le domaine social se constate partout. Récemment, à l'occasion d'une conférence qui se tenait à Inuvik, un délégué esquimau déplorait que « la famille esquimaude moyenne comprenne le père, la mère, les grands-parents, deux enfants, un sociologue et un anthropologue. »

On peut objecter que la collecte d'informations statistiques personnelles ne contribue pas directement au bien-être, mais il est plus difficile d'envisager un recul en ce domaine sans un retour à une société peu spécialisée et à faible rendement économique. La question de savoir si cela est souhaitable, ou si les informations statistiques qu'on recueille sont bien celles qu'il faut, dépasse le cadre de notre étude. Nous sommes partis de l'hypothèse que la structure sociale deviendra de plus en plus complexe au cours des prochaines années, et que cette tendance se traduira par un accroissement de la demande d'information statistique. Bien plus, des recherches s'appuyant sur les statistiques ont contribué à l'amélioration des conditions de vie de l'homme, dans certains cas. L'établissement d'un lien entre le cancer et l'abus du tabac par des moyens statistiques en est un bon exemple. L'amélioration des soins apportés aux personnes âgées, résultat d'une analyse statistique des dossiers médicaux dans une province de l'Ouest, en est un autre. Cette dernière étude a été faite à l'insu des personnes en cause. Là encore la violation du caractère privé de l'information personnelle a permis de réaliser un progrès. Comme dans nombre d'autres cas, il s'agit de faire la part du pour et du contre.

Comme beaucoup d'informations, qu'elles soient économiques ou sociales, présentent fréquemment un caractère personnel, il est clair que la collecte même des données constitue parfois une intrusion dans la vie privée. Cette intrusion pourra devenir intolérable, mais certains considèrent de plus en plus la visite d'un enquêteur comme une distraction au même titre que celle d'un représentant offrant ses produits.

D'ailleurs, les recherches de notre groupe d'étude soulèvent ce problème même qu'il avait pour mission d'examiner; l'enquête par questionnaire a engendré une multitude d'opérations statistiques, et l'étude des attitudes du public face à l'ordinateur, effectuée par le ministère des Communications, a suscité d'autres sondages et de nouvelles statistiques.

Si l'on met à part la question de la nature et de la quantité des

informations à recueillir, ainsi que celle des moyens de collecte, la principale préoccupation des statisticiens concerne la protection de l'information personnelle pendant sa manipulation ; ils savent qu'à moins de garanties contre les fuites, les sources tariront. Ce souci n'est pas universel. Les chercheurs qui ne font appel qu'une seule fois à leurs sources n'ont pas les mêmes motifs pour respecter scrupuleusement le caractère confidentiel de l'information. Ainsi, dans les bureaux d'études de marchés, on vise à la protection des clients plutôt qu'à celle des enquêtés.

Malgré leur souci presque unanime de protéger l'information confidentielle, les statisticiens se trouvent parfois en butte à des difficultés d'ordre pratique.

1. La divulgation par les statistiques [2]

La publication de statistiques établies par groupement d'unités de sondage peut donner lieu à la divulgation involontaire d'information confidentielle. Dans le cas le plus simple, la divulgation accidentelle est directe. C'est ce qui se produit quand un tableau comporte un article n'intéressant qu'une personne (physique ou morale) ou plusieurs articles avec prédominance manifeste de telle personne dans les totaux indiqués. I. P. Fellegi, de Statistique Canada, s'est livré à une étude approfondie de cette question et de quelques problèmes connexes. Le passage ci-après est tiré de son étude [3].

> « L'usage en statistique est de ne publier aucun résultat se fondant sur un échantillonnage de moins de trois enquêtés. C'est qu'en publiant les résultats relatifs à une unité ne comportant que deux enquêtés, l'identification mutuelle serait chose aisée ; chacun n'aurait qu'à soustraire du total les données de son propre rapport pour connaître les informations concernant l'autre. Ne sont pas non plus publiés les résultats relatifs à une unité de sondage de plus de trois enquêtés si les données fournies par un ou deux enquêtés dépassent une proportion déterminée du total. Cette précaution s'impose évidemment dans les cas de répartitions fortement asymétriques où le nombre des réponses ne constitue manifestement pas un critère sûr. »

Le problème de la divulgation par résidu est plus délicat. Elle se produit lorsqu'un ensemble de résultats statistiques peut être

manipulé arithmétiquement, et donner, par déduction, des informations sur un enquêté, même si aucun des tableaux n'en donne sur lui. Ainsi, il y a risque de divulgation par résidu quand, dans un tableau, une donnée, qui a été omise, peut être déduite des totaux et des autres données du tableau. Tout nouveau tableau, fondé sur les données de la même enquête, permet de déduire des informations confidentielles par comparaison avec les tableaux précédents. C'est pourquoi des mesures préventives s'imposent.

À côté des solutions théoriques compliquées, il existe une méthode simple fréquemment retenue pour résoudre ce problème. Elle consiste à modifier légèrement les données, c'est-à-dire à introduire des erreurs aléatoires très faibles que l'on retrouvera dans chaque tableau et dont on connaît les propriétés statistiques. De cette manière, il est impossible d'obtenir des informations ne prêtant à aucune équivoque sur une personne donnée, même si on l'a identifiée de façon certaine. Cette méthode, qui sera probablement adoptée par Statistique Canada, est à l'origine d'erreurs supplémentaires dans les résultats. Mais ces erreurs sont faibles par rapport aux autres types d'erreur qui existent déjà.

2. Statistique Canada

La principale activité de Statistique Canada, pour ce qui est de la population, est le recensement décennal. Des renseignements moins complets sont recueillis en outre au milieu de l'intervalle de dix ans. Les réponses au recensement individuel ne sont utilisées qu'à des fins statistiques, comme le stipule la Loi sur la statistique, et par conséquent ne peuvent être mises à la disposition de l'administration fiscale ou d'autres services administratifs ; d'autre part, ces réponses sont manipulées par un personnel assermenté et les données recueillies sont publiées sous une forme qui ne permet pas d'établir de rapport avec les personnes physiques ou morales sauf demande de leur part. Il se peut que la Loi sur la statistique assure aux Canadiens une protection qui n'existe pas aux États-Unis, faute d'une législation correspondante.

Des recenseurs assurent la distribution des imprimés. Ceux-ci seront vérifiés et mis sur microfilm pour deux fiches distinctes. La première, destinée à l'ordinateur, ne renferme les noms que sur la copie microfilmée : la bande de l'ordinateur ne renferme pas de noms en langage machine. La seconde, utilisée pour les recherches, ne porte que le nom, l'adresse et l'âge de l'enquêté (jusqu'au dernier recensement, ce deuxième exemplaire renfermait toutes les

informations). Une fois reproduits sur microfilms, les imprimés originaux sont détruits par déchiquetage.

Le Canada publie en outre 140 000 séries statistiques annuelles. Les informations individualisables font l'objet de nombreuses précautions : si des données doivent être traitées à l'extérieur, des membres du personnel en assurent eux-mêmes le transport et assistent au traitement.

De tous les organismes fédéraux, Statistique Canada est le seul, si l'on excepte le ministère du Revenu national, qui soit astreint, par son statut, à publier des informations tout en faisant respecter le caractère confidentiel des données recueillies. La loi prévoit des sanctions pour « toute personne qui, sans excuse légitime, ...refuse ou néglige de répondre, ou donne volontairement une réponse fausse à une question indispensable à l'obtention de renseignements que l'on cherche à obtenir pour les objets de la présente loi ». Elle stipule en outre ce qui suit : « nul, si ce n'est une personne employée ou censée être employée en vertu de la présente loi et qui a été assermentée en vertu de l'article 6, ne doit être autorisé à prendre connaissance d'un relevé fait aux fins de la présente loi ... [et] aucune personne qui a été assermentée en vertu de l'article 6 ne doit révéler ni sciemment faire révéler, par quelque moyen, des renseignements obtenus en vertu de la présente loi de manière qu'il soit possible, grâce à de telles révélations, de rattacher à un particulier, à une entreprise ou à une organisation identifiables, les détails obtenus dans un relevé qui les concerne exclusivement ».

Dans le reste de l'article, le législateur précise les cas où la révélation est permise, notamment : la divulgation à un organisme provincial de statistique, à la discrétion du ministre (pourvu que soit strictement respecté le caractère confidentiel de l'information) ; la divulgation d'information quand les intéressés ont au préalable donné par écrit leur consentement ; la divulgation d'informations, qui, aux termes d'une loi, présentent un caractère public.

Toutes les informations obtenues d'autres organismes sont traitées suivant les règles du secret qui s'y appliquent à la collecte. Cette conduite est si bien connue que certains agriculteurs, tellement convaincus que leurs informations ne sortiraient pas de Statistique Canada, avaient inscrit la marijuana dans la catégorie des « autres cultures » sur un imprimé.

Étant donné le volume des données et toutes les manipulations qu'elles exigent, Statistique Canada doit recourir largement à l'ordinateur. Le traitement de l'information s'effectue sur place

pour une bonne part, et l'accès à l'ordinateur fait l'objet d'une surveillance très étroite.

3. La recherche en sciences sociales [4]

Dans le domaine des sciences sociales, la recherche tend à se centraliser et à s'appuyer sur des enquêtes de plus en plus concentrées, et dont certaines comportent l'utilisation de modèles statistiques exigeant des quantités considérables de données. Ces phénomènes ont hâté l'avènement de l'ordinateur comme outil indispensable des sciences sociales. Non seulement il y a eu, pour diverses raisons éducationnelles, accroissement du nombre des professeurs et des étudiants pratiquant la collecte d'informations, mais aussi de profonds changements dans les méthodes de manipulation des informations ; souvent celles-ci sont transférées du questionnaire à une bande magnétique, à un chargeur de plastique, à un microfilm ou à une microfiche. Une fois stockée sous forme assimilable par l'ordinateur, l'information est beaucoup plus facile à extraire et se prête mieux aux corrélations.

Certains chercheurs utilisant des procédés de collecte discutables, la question de la préservation du caractère confidentiel de l'information se pose. De plus, beaucoup d'informations ne sont pas seulement personnelles au sens où on l'entend habituellement, mais se rapportent à des actes ou des métiers illicites, telles la consommation de drogues ou la prostitution. Même si les informations communiquées comportent habituellement l'engagement d'une discrétion absolue, on peut se demander si elles ne risquent pas d'être mises à la disposition de la Justice par assignation. L'*American Council of Education* a résolu ce problème en se servant d'un numéro de code pour identifier ses dossiers personnels ; le fichier de correspondance entre noms et numéros est gardé dans un pays étranger (le Canada, en l'occurrence) ; aussi les dossiers ne sauraient faire l'objet d'une assignation ou d'une saisie.

Les universités et les organismes de recherche répugnent généralement aux contrôles de l'extérieur. L'autre solution, c'est-à-dire l'autoréglementation, n'est pas fréquente. Pourtant l'*Institute for Behavioural Research of York University* a adopté un code déontologique et applique des mesures de sécurité semblables à celles de Statistique Canada.

En juillet 1971, une enquête tendait à déterminer combien de comités de déontologie s'intéressant à la recherche en sciences

humaines existaient déjà ou étaient en projet. Des lettres ont été adressées aux directeurs des sections de sociologie d'un certain nombre d'universités canadiennes ; d'après les dix-huit réponses, il y en avait quatre, dont l'un n'avait d'autorité que sur la section de sociologie. Quatre autres universités formaient des projets en ce domaine. Les réactions à l'idée de créer de tels comités étaient très variables. Certains la trouvaient excellente ; d'autres la rejetaient carrément. L'un des adversaires s'est exprimé en ces termes : « Comme chercheur et professeur de méthodes de recherche, je serais le premier à m'opposer à la création de pareil comité ».

Aux États-Unis, la *Russell Sage Foundation*, qui accorde un soutien financier abondant pour les recherches sociologiques, exerce une certaine surveillance. En accordant des bourses, elle exige des titulaires qu'ils respectent son code déontologique, qui prescrit le respect de la vie privée. Il n'existe rien de semblable au Canada. Les organismes fédéraux subventionnant la recherche pourraient donner l'exemple.

4. Les bureaux d'études des marchés

Le Groupe avait projeté un entretien avec un important bureau d'études des marchés, mais en a été empêché pour des raisons d'ordre administratif. Et faute d'assez de réponses de ce type d'entreprises à son questionnaire, il n'a pu tirer de conclusions sur leurs méthodes et pratiques. Cependant, un conseiller a écrit, sans preuve à l'appui, que les normes de sécurité y sont moins rigoureuses que dans les universités, ou déjà elles sont inférieures à celles des organismes de l'État. En fait, les activités de ces bureaux ne se limitent pas aux études des marchés ; elles embrassent notamment les sondages d'opinions politiques (tels ceux de l'Institut Gallup qui sont publiés régulièrement) et les enquêtes sur les attitudes.

[1] DRUCKER, Peter F., « The Age of Discontinuity », Harper and Row, New York, 1968, 383 pages.

[2] Notre exposé sur la divulgation des statistiques et sur Statistique Canada s'inspire largement de l'étude effectuée pour notre Groupe par H. S. Gellman et intitulée *Statistical Databanks and Their Effects on Privacy.*

[3] FELLEGI, I. P., *On the Question of Statistical Confidentiality,* « Proceedings of the Social Statistics Section, American Statistical Association, », 1970, p. 7.

[4] Notre exposé sur la recherche sociale s'inspire largement du rapport rédigé par T. McPhail pour le ministère des Communications et intitulé *Social Science Research and the Rights of Human Subjects.*

Chapitre 4
Les cadres administratifs

De tous les utilisateurs d'information personnelle, les cadres administratifs forment la classe la plus nombreuse. En général, le cadre administratif ne recherche pas d'informations sans rapport avec les décisions à prendre. Il ne se sent pas obligé de respecter le caractère confidentiel des informations, comme le statisticien. De plus, il tend vers les moyens les plus simples de se renseigner. Plutôt que de poser des questions embarrassantes pour recueillir certaines données, il fera appel à une source anonyme. C'est ainsi que s'établissent des réseaux d'échange de renseignements personnels, où l'on échappe aux règles concernant l'information confidentielle. À la limite, une organisation fera passer l'un de ses employés à une autre organisation à des fins de liaison.

Le pouvoir sur les individus confère aux cadres administratifs plus de liberté qu'il ne serait souhaitable. Ce phénomène est flagrant dans les relations entre assistants sociaux et bénéficiaires de prestations, ainsi qu'entre employeurs et employés, mais il semble que peu de gens veuillent s'attaquer à cette situation de fait, non plus qu'à d'autres moins délicates d'ailleurs.

Ce chapitre et le suivant exposent les règles suivies par les cadres administratifs dans différents secteurs.

1. Les employeurs

Au moment de pourvoir à une vacance, les employeurs réunissent des informations sur les candidats qui se présentent. Par la suite, ils ajoutent des éléments aux dossiers des employés en vue de décisions touchant les promotions et les licenciements. Les dossiers des anciens employés serviront à la gestion des caisses de retraite.

Pour les vérifications sur un candidat à un poste, l'employeur s'adressera généralement à une agence de renseignements commerciaux. La quantité des informations varie selon l'importance du poste à pourvoir. Parlant de l'embauche des travailleurs manuels, un directeur de compagnie déclarait au cours d'une entrevue : « Nous rassemblons juste assez de renseignements sur eux pour les payer ». Par contre, les candidats à un poste de cadre supérieur font l'objet d'une enquête approfondie.

Les postes exigeant un contrôle sécuritaire supposent des renseignements préliminaires encore plus précis. La vérification embrasse alors les empreintes digitales, les changements d'adresse successifs, les renseignements personnels sur les proches parents. Quand la sécurité nationale est en cause, ces données servent aux recherches de la Gendarmerie royale du Canada.

D'après les réponses au questionnaire, l'automatisation est réalisée à 40 p. 100 pour les fichiers du personnel de 500 articles ou moins et à 76 p. 100 pour ceux de plus de 500. Les aptitudes des fonctionnaires sont consignées sur leur demande par la Commission de la fonction publique du Canada dans un fichier automatisé dit Permatri. Cette banque d'information est accessible au personnel autorisé par 32 terminaux répartis dans les ministères. L'utilisateur doit s'identifier et donner un mot de passe, mais l'information qu'il obtient et l'utilisation qu'il en fait ne sont pas enregistrées. Les dossiers de 32 p. 100 des fonctionnaires fédéraux, soit 69 000, se trouvent dans cette banque. La plupart appartiennent à la catégorie des administrateurs, spécialistes et assimilés. L'information de base (nom, adresse, traitement et poste) figure toujours dans la banque, mais l'employé peut décider s'il convient d'y consigner le détail de sa carrière et de ses aptitudes. Il faut noter cependant que les banques du genre de Permatri constituent l'exception.

La majorité des employés ont le droit de voir leur dossier et de le contester ; toutefois un grand nombre d'employeurs voudront savoir le mobile de l'employé avant de lui accorder l'accès à son dossier. Dans le cas des employés syndiqués, la nature des

renseignements et les modalités d'accès sont souvent régies par la convention collective. De plus, divers employeurs ont cessé de recueillir des informations touchant la nationalité d'origine ou la religion, au cas où elles entraîneraient une certaine discrimination.

Les employeurs constituent l'une des plus importantes sources d'information sur les personnes. C'est à eux que s'adressent d'abord les agences de renseignements commerciaux tout comme les établissements d'enseignement et les employeurs éventuels. De plus en plus, les employeurs se limitent à des confirmations de services, sauf à la requête expresse de leurs employés. Toutefois, une certaine catégorie d'employeurs, dont les banques, les compagnies d'assurances, les grands magasins, les bijoutiers et les fourreurs, doivent collaborer avec la police selon leur intérêt commun.

Même les chômeurs figurent dans les fichiers automatisés. Le ministère fédéral de la Main-d'œuvre et de l'Immigration met au point un fichier automatisé qui permettra d'obtenir instantanément un état à jour des demandes d'emploi, avec indications des antécédents professionnels et descriptions des tâches. Le Ministère, grâce à cet instrument, devrait être beaucoup mieux en mesure d'établir des correspondances entre postes à pourvoir et offres de services.

2. L'octroi des crédits

Le crédit conditionne l'économie. Dans le cadre du présent rapport, il ne nous appartient pas d'apprécier les incidences sociales de ce phénomène ni les autres évolutions possibles, mais il est sûr que la dépendance à l'égard du crédit tend toujours à s'accentuer. Au Canada, le crédit à la consommation a quintuplé au cours des deux dernières décennies ; en 1971 il atteignait les $ 9 milliards. Il s'agit essentiellement de crédit immobilier, de crédit mobilier, de petits prêts, de cartes de crédit bancaires, de cartes de crédit voyage-distraction, de cartes de compagnies pétrolières et de paiements différés quant aux grands magasins. Comme les banques ont un rôle particulier et prépondérant, nous en traiterons à part dans le prochain chapitre.

L'importance du secteur crédit étant manifeste, le Groupe d'étude s'est intéressé principalement à deux aspects de cette activité économique. D'abord, la plupart des établissements de crédit recherchent le maximum d'information possible sur ceux qui s'adressent à eux. Ensuite, les personnes qui consomment à crédit laissent des traces de leurs dépenses à l'hôtel, dans les boîtes de

nuit, sur leurs parcours en voyage, et à l'occasion d'emprunts hypothécaires ou autres... Le secteur du crédit repose sur l'information, qui est devenue l'une de ses activités.

Le crédit suppose toujours un échange, ainsi que la Banque royale du Canada, dans son mémoire au Groupe d'étude, le faisait ressortir en ces termes : « Celui qui présente une demande de prêt à une banque consent, pour établir sa réputation de solvabilité, à fournir des renseignements sur sa personne et ses antécédents pécuniaires[1]. Toute information que la banque reçoit est considérée comme appartenant au client et, de ce fait, présente un caractère confidentiel. » Certains établissements de crédit prennent eux-mêmes les décisions de prêts, mais un grand nombre font appel à des entreprises spécialisées, dont les agences de renseignements commerciaux, les fichiers centraux de créances, et les services de surveillance des cartes de crédit. On a moins recours aux agences d'enquêtes commerciales.

Dans certaines provinces, le ministère de la Justice a mis sur pied des systèmes automatisés d'enregistrement de la propriété afin de combattre la vente frauduleuse de biens sur lesquels pèse une créance privilégiée. La plupart des données concernent des achats de voitures à crédit. Toutes sont accessibles à quiconque au tarif de $ 2 l'unité.

La *Canadian Consumer Loan Association* est le centre d'information des petits établissements de crédit. Elle tient des dossiers grâce auxquels on peut s'assurer que le plafond de crédit n'est pas dépassé, ou s'il y a défaillance. Le *Credit Index* de Morristown (New Jersey), accessible par télétype, renferme des informations sur neuf millions de défaillants, dont la dette globale s'élève à un demi-milliard de dollars; 8 500 personnes de ce répertoire résident au Canada.

En règle générale, les banques s'appuient sur l'analyse des relations avec leurs clients pour décider des prêts; mais il leur arrive aussi de se renseigner auprès d'autres banques, d'agences de renseignements commerciaux ou de l'employeur de leur client. Les banques respectent rigoureusement le caractère confidentiel des informations, sauf sous la contrainte de la loi ou avec le consentement exprès ou tacite de leur client. Toutefois, une banque pourra fournir à une agence de renseignements commerciaux, sur demande, une appréciation de solvabilité à l'occasion d'un prêt personnel sans garantie. Les indications portent sur le plafond de crédit, le dossier des versements, le solde des prêts et le temps depuis lequel durent les relations avec la banque.

En *Common law*, les relations entre une banque et ses

déposants sont confidentielles ; la première s'exposerait à des poursuites en divulguant le compte de ses clients, mais pour obtenir gain de cause, les seconds devraient prouver qu'ils ont été lésés.

L'exploitation des cartes de crédit *Chargex* et *American Express* et des cartes des compagnies pétrolières, entre autres, repose largement sur les ordinateurs pour la mise à jour constante des comptes et la prévention des usages frauduleux des cartes. Dans bien des cas, les personnes autorisées à l'acceptation des cartes bénéficient d'un accès immédiat aux fichiers automatisés. Normalement, l'ordinateur indique si la carte a été volée et si le titulaire est solvable.

Nombre de cartes de crédit ont cours dans toute l'Amérique du Nord. La vérification du crédit est organisée en fonction du traitement des données concernant les titulaires canadiens de cartes, qui s'effectue aux États-Unis pour une bonne part. Ainsi, pour certaines cartes de compagnies pétrolières, l'information est enregistrée à la *National Data Corporation of Atlanta*, en Georgie, avec liaison à Toronto par terminal.

L'*American Express* (avec 130 000 fiches sur des Canadiens dans sa banque d'information) est sans doute la première, sous ce rapport, aux États-Unis. Ses informations sont presque uniquement de nature comptable. D'autres organisations œuvrent dans des domaines analogues : le *Diners Club* (avec environ 75 000 membres canadiens), la Carte Blanche (avec environ 14 000) et *American Airlines* (avec 1 500 Canadiens, pour la plupart de la région de Toronto).

On a souvent souligné que les gros utilisateurs de cartes de crédit laissaient des traces de leur passage propres à servir à la police ou à d'autres. Il est arrivé que des arrestations en résultent.

3. L'imposition

Un grand nombre de Canadiens considèrent le revenu comme affaire personnelle. Pourtant, la plupart des salariés sont tenus de le déclarer au percepteur.

Le ministère du Revenu national (Impôt) perçoit l'impôt fédéral sur les revenus des particuliers et des sociétés, les contributions aux fonds de retraite du Canada et les primes d'assurance-chômage. Il perçoit aussi l'impôt provincial sur le revenu, sauf pour le Québec. Le personnel de ce ministère est tenu au secret et passible d'une amende pouvant s'élever à $ 1 000 au maximum pour divulgation d'informations sur les contribuables à des personnes non autorisées à cet effet.

Deux cent trente personnes travaillent au traitement des données; pendant les périodes de pointe, elles sont assistées de 1 000 perforatrices temporaires. La perforation alphabétique (par exemple du nom et de l'adresse) et la perforation numérique (du montant des impôts payés, par exemple) sont exécutées par des groupes distincts. Le rendement que l'on exige de ces employées est tel qu'il leur serait pratiquement impossible de lire une information, et à plus forte raison, de la retenir.

Les principaux fichiers automatisés sont :

- Le grand fichier des contribuables, qui comprend 10 500 000 dossiers de 500 caractères chacun, enregistrés sur 125 bobines magnétiques. Celles-ci étant établies en trois copies, on pourrait reconstituer le grand fichier s'il était effacé par inadvertance ou intentionnellement;
- le fichier comptabilité et perception des impôts des particuliers, qui peut comprendre jusqu'à 1 500 000 articles de 400 caractères chacun;
- le fichier des déductions à la source par l'employeur (500 000 articles de 300 caractères chacun);
- le fichier des renseignements supplémentaires T-4 (15 000 000 articles de 40 caractères).

Les organismes ou les personnes ci-après peuvent aussi recevoir des données de déclarations d'impôts :

- Statistique Canada, qui a accès aux déclarations d'impôts d'entreprises en vertu de la loi de 1965 sur les déclarations des corporations et des syndicats ouvriers. Cet organisme a également accès aux déclarations de certaines catégories de particuliers en vertu de la loi de 1971 sur la statistique.
- Les procureurs de la Couronne quand ils ont besoin d'information pour des poursuites dans les cas de fraude fiscale[2].
- Les neuf provinces pour lesquelles les impôts sont perçus. Le Québec, qui tient ses propres archives d'impôts, peut se servir des déclarations de revenus pour la vérification des ressources pécuniaires et pour l'examen des demandes de bourse d'études. Les autorités estiment que le gouvernement du Québec économise ainsi $ 6 millions par année. Cette vérification n'est pas possible dans les autres provinces, car

les informations fiscales transmises par le gouvernement fédéral ne peuvent servir qu'à des fins statistiques d'après la Loi de l'impôt sur le revenu.

- Les feuillets concernant les ressortissants américains sont envoyés à l'*Internal Revenue Service* en échange de renseignements équivalents sur les Canadiens résidant aux États-Unis, conformément aux dispositions d'un traité.
- Tout contribuable peut voir sa feuille d'impôt au Bureau régional en produisant une preuvre de son identité ou autoriser un représentant à cet effet.

La division de l'Impôt doit mettre sur pied un système de télécommunication qui donnera à ses vingt-huit bureaux régionaux accès aux informations fiscales centralisées à Ottawa.

4. L'assurance-vie

L'escroquerie aux dépens des compagnies d'assurance se pratique dans le monde depuis au moins un siècle si l'on en juge par les mesures qu'elles ont prises contre les déclarations mensongères et les réclamations frauduleuses. En règle générale, les compagnies d'assurance doivent recueillir une grande quantité d'informations pour souscrire les polices et régler les réclamations. Ces informations sont consignées dans des fichiers manuels. Les informations sur le paiement des primes et les modifications des contrats sont souvent traitées par ordinateur. Dans ce secteur, dont l'activité s'exerce sur une grande échelle, l'ordinateur occupe une place importante depuis longtemps déjà.

En assurance-vie, le proposant commence par donner des renseignements à son agent qui les transmet au siège social de la compagnie. Il doit en général indiquer ses antécédents médicaux et signer un désistement autorisant la compagnie à demander des renseignements aux établissements de santé ou aux médecins qui ont un dossier sur lui. Peut-être aussi devra-t-il passer un examen médical ; alors le rapport du médecin constituera un élément de la proposition.

Le *Medical Information Bureau* (M.I.B.), de Boston, joue un rôle important dans le dépistage des propositions entachées de fraude ou comportant un risque excessif. Il s'agit d'une association de 700 compagnies d'assurance sur la vie, dont 80 canadiennes. Le Bureau a pour fonction de signaler aux assureurs les maladies et les risques déjà constatés par d'autres assureurs et que le proposant n'aurait pas mentionnés. Lorsque l'assureur refuse une demande

ou déclasse le candidat en raison d'une maladie grave, il en avise le Bureau par message codé ; la décision finale de la compagnie n'est pas transmise. Les résultats d'un examen médical qui peuvent indiquer une amélioration sont parfois communiqués au Bureau.

Toutefois tout genre d'information peut faire l'objet d'un rapport au Bureau. Quelque 90 p. 100 des rapports renferment une information médicale codée et 10 p. 100 des données d'un autre ordre. Chaque année, le Bureau reçoit un million et demi de rapports des compagnies membres (une compagnie canadienne en fournit 1 000 par mois) et répond à dix-huit millions et demi de demandes de renseignements. Le Bureau affirme posséder des renseignements codés sur 800 000 Canadiens dans des fichiers distincts.

La plupart des demandes d'assurance-vie donnent lieu à une vérification par une agence d'enquêtes commerciales, qui s'adressera parfois au proposant lui-même et, presque toujours, à ses voisins, à ses employeurs présents ou passés. Cette agence essaie de déterminer si le sujet boit de façon excessive, mène une vie de débauche, s'il est lié à des gens peu recommandables, ou encore s'il pratique, par exemple, la plongée sous-marine, le parachutisme ou l'aviation sportive. La rigueur de l'enquête est fonction du montant en cause. Dans le cas des polices importantes, la compagnie confiera l'investigation à un enquêteur expérimenté, et le rétribuera largement.

En général, le candidat à l'assurance-vie ou à l'assurance-maladie sait qu'il y aura enquête pour déterminer s'il est assurable. Dans la plupart des cas, l'autorisation de procéder à l'enquête est incorporée à la partie de la proposition en caractères fins. Au Canada, les demandes d'assurance-vie sont presque toujours acceptées. Dans un mémoire au Groupe d'étude la *Canadian Life Insurance Association* a révélé que 97 p. 100 des demandes avaient été acceptées en 1969. Quelque 1 p. 100 ont été refusées pour faiblesse cardiaque, et un peu moins pour diverses maladies graves. Quant au reste, un refus sur quinze avait pour motif une activité professionnelle dangereuse.

Souvent, la proposition d'assurance-incendie ou d'assurance-automobile donne lieu aussi à une enquête. Le *Fire Underwriters Investigation Bureau* de Montréal tient à jour une liste des réclamations pour incendie, vol et autres sinistres. Les bureaux des véhicules automobiles fournissent sur demande les renseignements contenus dans leurs fichiers, y compris les infractions et les condamnations. Au Manitoba, le directeur du bureau provincial de

l'assurance-automobile a accès aux informations contenues dans les fichiers du gouvernement.

5. L'éducation

Quant au traitement de l'information sur les étudiants, aucune politique formelle n'est à l'horizon au Canada, si ce n'est en Ontario, où l'on a présenté récemment un projet de loi sur cette question. Dans les réponses au questionnaire du Groupe d'étude, plus du cinquième des enquêtés ont noté que des établissements d'enseignement leur avaient fourni des informations sur des étudiants.

Il est ressorti d'une enquête menée dans les universités de l'Ontario, en 1970, que seulement deux établissements avaient une politique quant à la manipulation des dossiers des étudiants.

Le caractère personnel des dossiers des étudiants s'entend de différentes façons suivant le cadre et les traditions. Ce qui est considéré comme une atteinte flagrante à la vie privée dans telle université sera la norme dans une autre. Des consignes très strictes sont appliquées dans certains établissements pour que les notes restent tout à fait confidentielles. Ailleurs, des listes de notes circulent dans toute la faculté, sont affichées sur un tableau, publiées par des journaux et même, dans un cas, communiquées publiquement par le doyen.

Des groupes d'étudiants ont protesté contre la collecte par des universités d'informations concernant le caractère ethnique, la religion, la nationalité ou l'origine sociale; ils craignaient qu'un jour l'administration n'utilise ces données à des fins discriminatoires. Or, les personnes ou les groupes à l'origine de ces démonstrations voudront peut-être savoir un jour combien d'autochtones sont admis aux études supérieures, combien de non-catholiques fréquentent telle université autrefois officiellement catholique et relevant aujourd'hui du ministère de l'Éducation provincial, combien de personnes issues de la classe ouvrière sont incrites à l'université, combien d'Américains sont inscrits au second cycle.

En règle générale, les universités diffusent deux sortes d'information : les dossiers des études et les lettres de recommandation. Les premiers consistent ordinairement en photocopies de fiches permanentes sur lesquelles sont apposés des articles-labels indiquant les numéros de cours, les unités de valeur et les notes obtenues. Souvent, s'ajoute le dossier du secondaire. Ce genre de document peut être envoyé à l'employeur ou à l'organisation qui le réclame, à la demande de l'étudiant.

L'automatisation des dossiers est envisagée pour les écoles élémentaires et secondaires à l'échelon régional. Cette conversion n'ira pas sans difficultés toutefois, car très souvent dans les dossiers des élèves, les conseillers consignent des informations personnelles à structure non imposée; or ces données, qui occupent une place importante, seraient largement éliminées par l'automatisation.

Le gouvernement ontarien a présenté, en mai 1972, un projet de loi qui prévoit pour les élèves, et les parents des élèves de moins de 18 ans, l'accès aux dossiers scolaires; celui-ci serait interdit cependant aux employeurs, à la police et aux tribunaux.

On est fondé à croire que les revenus déclarés dans les demandes de bourses aux universités des provinces sont fréquemment inférieurs à la réalité. Certaines provinces se sont dotées d'un organisme central, qui reçoit les demandes et les soumet à un premier contrôle afin de déterminer si le candidat satisfait à toutes les conditions. Généralement le revenu indiqué sert de critère à cette étape. Un échantillon des demandes (pouvant atteindre 25 p. 100) est prélevé en vue d'une vérification plus approfondie.

Les administrateurs des régimes de bourses estiment qu'il serait profitable de vérifier les demandes de bourses en se référant aux déclarations de revenu pour fins d'impôt, mais ce contrôle n'est possible qu'au Québec. Dans cette province, nous le rappellerons, le dépistage des demandes frauduleuses permet de réaliser une économie de $ 6 millions par an, d'après les autorités.

Les demandes refusées ou trouvées douteuses sont envoyées aux responsables des bourses dans les établissements d'enseignement pour une enquête. Le zèle des responsables est très variable. Certains font beaucoup de recherches, d'autres se contentent d'accepter les déclarations de l'étudiant. Pour confirmer les renseignements se rapportant au revenu des parents ou à celui de l'étudiant, ils ont la ressource de demander des documents comme les feuilles T-4 ou une copie de la déclaration d'impôt T-1, ou quand les parents sont dans les affaires, le bilan d'un expert-comptable.

6. Les agences de renseignements commerciaux

Les agences de renseignements commerciaux sont aussi, en certains cas, des agences d'enquête. Les principaux clients de celles-ci ne sont pas en fait les établissements de crédit, mais les

compagnies d'assurance-vie, incendie ou automobile et les employeurs; les établissements de prêt sur hypothèque et dispensateurs de cartes de crédit voyage-distraction font aussi appel à leurs services.

Les agences de renseignements commerciaux proprement dites ne font pas d'enquêtes, en règle générale. Elles obtiennent leurs informations de leurs clients, en grande partie, soit des grands magasins, petits établissements de prêts et petites entreprises qui pratiquent le crédit. Les compagnies pétrolières et les banques ont aussi recours à leurs services, mais dans une moindre mesure. Les agences de renseignements commerciaux ne font pas, à vrai dire, de gestion administrative; toutefois elles offrent un type de service administratif, à information centralisée. C'est la raison pour laquelle nous en traitons dans ce chapitre.

Il existe un grand nombre d'agences de renseignements commerciaux indépendantes, dont la plupart (151) sont membres de l'*Associated Credit Bureaus of Canada.* Elles réalisent des bénéfices bruts de $ 12 à $ 15 millions par an, et occupent quelque 2 000 personnes. Le prix moyen des rapports est de $ 1,35

Les membres de l'*Associated Credit Bureaus of Canada* souscrivent à un code déontologique et à des principes de protection de la vie privée, qui englobent bon nombre des droits énoncés aux États-Unis dans le *Fair Credit Reporting Act* de 1970. Il faut dire que l'association canadienne entretient des liens avec l'*Associated Credit Bureaus Inc.* des États-Unis, et que les fiches de renseignements se déplacent librement entre les deux pays.

Les agences de renseignements commerciaux, au Canada, n'emploient pas encore les ordinateurs mais elles envisagent l'automatisation, poussées par une demande de services mieux adaptés et plus complets. Mais, pour d'aussi petites entreprises, la transformation serait onéreuse. Plusieurs agences américaines, dont *Credit Data* et *Retail Credit Corp.*, ont déjà automatisé leurs fichiers; il est donc possible que les agences canadiennes louent un système de programmation d'une société américaine pour l'exploiter sur ordinateur au Canada. Toutefois, même avec ce moyen la conversion coûtera très cher. Or, sans cet effort de modernisation, les agences risquent que des clients se tournent vers d'autres sources.

Le *Retail Credit of Canada*, filiale de la *Retail Credit Corporation of Atlanta*, (Georgie), qui pratique surtout l'enquête, a ajouté à ses activités la simple fonction de renseignements exposée plus haut. Au Canada, elle assure actuellement quelque 30 p. 100 de ce service.

Souvent on a formé le vœu que les agences de renseignements commerciaux soient tenues d'aviser les sujets de chaque consultation de leur dossier. Les agences objectent que la plupart de ceux qui demandent du crédit savent que leur dossier sera consulté et que pareille pratique serait prohibitive. Même une augmentation de 10 p. 100, soit 14 ¢ par renseignement, aurait des répercussions fâcheuses sur le chiffre d'affaires ; elle éloignerait des clients qui traitent déjà avec les agences d'enquête, dont les rapports sont plus chers ($ 5 par renseignement), mais contiennent des informations plus complètes ; ou encore, elle les amènerait à suivre, pour l'octroi du crédit, un ensemble de règles arbitraires faisant intervenir l'âge, la profession et les années de résidence à telle adresse. Dans ces conditions, l'emprunteur devrait assumer cette hausse de frais, ou le crédit serait refusé pour des raisons arbitraires.

Ces considérations sont à retenir. Toutefois, il est douteux que la majorité des gens qui font une demande de crédit prévoient qu'on consultera à leur sujet une agence de renseignements commerciaux. Et, à supposer que l'existence de dossiers sur leur compte leur soit connue, ils ignoreraient fort probablement comment en prendre connaissance.

Il serait sans doute coûteux pour les agences d'avertir les intéressés à chaque consultation de leur dossier. Un moyen terme consisterait à le faire à la première, puis à tenir un état des consultations ultérieures dont on pourrait prendre connaissance sur demande. Le droit d'accès devrait avoir pour corollaire celui d'en corriger les inexactitudes et de recourir à un mécanisme en cas de litige. Actuellement, les membres de l'*A.C.B.* du Canada autorisent l'examen des dossiers et leur correction par les intéressés.

7. Le commerce des répertoires d'adresses

Le commerce des répertoires d'adresses n'est pas immédiatement lié à la question de la vie privée. Pourtant, nombre de gens considèrent qu'on porte atteinte à leur vie privée si on leur expédie du « courrier de dernière classe » après qu'ils ont assisté à une conférence, se sont abonnés à une revue ou ont fait immatriculer leur voiture. D'autre part, pour bien des gens, en particulier parmi ceux qui sortent peu, ce genre de courrier représente une distraction, sinon une source d'informations utiles.

Divers bureaux provinciaux des véhicules automobiles, depuis un certain temps, vendent des répertoires d'adresses de titulaires de

permis à raison de 1 ¢ l'unité. Au Manitoba, le prix a été porté à 10 ¢ le nom. Toutefois, plusieurs provinces s'interrogent sur cette pratique, qui a été fort critiquée.

Certains éditeurs de revues spécialisées offrent des répertoires d'adresses très au point, comportant, outre les informations de base sur le souscripteur, des renseignements particuliers, recueillis par des services d'enquête sur les lecteurs. Diverses associations font un usage analogue de leur liste de membres.

Il n'y a que demi-mal quand les adresses sont obtenues par contact direct, mais parfois les conséquences seront fâcheuses. Citons le cas d'une jeune femme enceinte dont le nom avait été porté sur un répertoire du fait de soins prénataux, et qui a reçu d'une banque un message de félicitations vers la date prévue pour la naissance ; or, elle avait fait une fausse couche entre-temps. Les listes d'envoi pour les écrits pornographiques sont établies parfois d'après des sources à peine imaginables. Telle personne a été inscrite sur pareille liste pour avoir commandé un livre sur l'élevage des chevaux à une maison spécialisée dans la liquidation des stocks d'éditeurs.

Un membre du Congrès, du nom de Gallagher[3], dans une lettre publiée par la revue *Computers and Automation,* citait une lettre reçue par le *San Francisco Suicide Prevention Service :*

> Cher Monsieur Suicide ... un abonnement serait la meilleure façon de contribuer au progrès pécuniaire de la famille Suicide.

Il se servait de cet exemple de production par ordinateur de courrier « personnalisé » pour faire valoir son projet de loi sur la publicité postale de mauvais aloi. Son projet touche essentiellement quatre questions :

- l'enregistrement des « courtiers » en répertoires d'adresses ;
- la possibilité pour chacun d'être épargné par le courrier en vrac, sauf s'il s'agit d'envois par des organisations de bienfaisance à but non lucratif ;
- la possibilité pour chacun de faire retirer son nom d'un répertoire d'adresses ;
- l'obligation, pour l'expéditeur, d'indiquer sur tout envoi comment il s'est procuré l'adresse du destinataire.

L'ordinateur permet de donner assez facilement satisfaction à ceux qui ne veulent pas recevoir de courrier publicitaire. À la réception du premier envoi, il leur serait loisible d'indiquer leurs intentions à cet égard, – pourvu qu'un imprimé leur offre

l'occasion de signifier leur choix. Une fois les données introduites dans l'ordinateur, il ne resterait qu'à dresser des listes d'envoi ne comprenant que les noms des personnes consentantes. Cette solution, que certaines organisations ont adoptée, devrait être satisfaisante pour tout le monde. En effet, le répertoire d'adresses aurait plus de valeur pour celui à qui il appartiendrait et aussi pour ceux qui l'exploiteraient, car il constituerait un outil publicitaire plus rentable.

1. La collecte d'informations d'ordre financier semble de règle dans plusieurs banques même si les prêts sont entièrement garantis, alors que ces renseignements semblent superflus en pareils cas.

2. Dans une cause récente devant le Cour de l'Échiquier, il a été révélé que des renseignements relatifs aux déclarations d'impôt sur le revenu d'un fonctionnaire fédéral avaient été communiqués à la « Couronne » sans raisons de fraude fiscale. Dans son arrêt, le juge s'est explicitement abstenu d'apprécier en droit la communication de ces renseignements, estimant que cette question débordait la compétence du tribunal et que les informations ainsi divulguées n'avaient rien à voir avec sa décision.

3. GALLAGHER, Cornelius E., « Computers and Automation », vol. 20, n° 4, avril 1971, p. 35.

Chapitre 5
Les banques et la médecine

Les fichiers des banques et des médecins peuvent être considérés comme d'un type administratif particulier. Toutefois, en raison du caractère strictement personnel des informations qu'ils contiennent, et aussi des incidences de l'informatique sur leur manipulation, nous avons jugé bon d'en traiter à part.

Dans ces deux domaines, bien sûr, les problèmes se posent différemment. La médecine avait pour assise le rapport traditionnel entre malade et médecin. Or, elle est en voie de passer à la formule de l'équipe. De plus, des problèmes nouveaux surgissent avec la gratuité des soins et la prolifération des informations comptables qui en résulte. Pour les banques, le problème est différent. Chaque année la masse des imprimés administratifs augmente de 7 p. 100 et le personnel chargé de leur manipulation exige des appointements plus élevés. Déjà les banques sont très engagées sur la voie de l'automatisation, et il est certain que le mouvement s'intensifiera. Actuellement, leurs frais à ce titre forment 7 p. 100 du total pour le Canada.

1. Les banques d'information des banques [1]

Pour les transferts de fonds, on se sert le plus souvent de chèques bancaires. En 1969, au Canada, le nombre des chèques établis a été de 1,25 milliard, et l'on prévoit qu'il augmentera de 7 p. 100 par an jusque vers 1980. On estime qu'un chèque est manipulé quatorze fois en moyenne au prix de 13¢ pour la banque. Il serait possible, toutefois, de réduire ces dépenses en simplifiant l'échange monétaire.

Depuis dix ans, les banques ont recours à l'ordinateur pour accélérer le traitement des chèques. Au Canada, l'automatisation a commencé en 1963 avec l'utilisation de trieuses rapides et des impressions codées sur les chèques. Ces machines lisent les codes, trient les chèques par numéro de compte et fournissent directement les informations (numéro de compte et montant) à un ordinateur qui produit un relevé mensuel pour le client.

Ces tâches sont maintenant automatisées dans 60 p. 100 des succursales des banques canadiennes privilégiées. Quelque 450 succursales de banques et de sociétés de gestion se servent de terminaux à clavier – reliés à des ordinateurs centraux par ligne téléphonique – grâce auxquels on peut inscrire les dépôts et les retraits, ainsi que mettre à jour les comptes d'épargne. La Banque de Montréal devrait disposer d'ici 1975 d'un vaste réseau téléinformatique reliant toutes ses succursales à un grand centre informatique. On estime qu'en 1977 jusqu'aux trois quarts des succursales de banques canadiennes devraient être en liaison directe avec des ordinateurs.

Les ordinateurs ont permis d'accélérer le mouvement des documents, mais non d'en réduire la quantité dans le secteur bancaire. Depuis une vingtaine d'années, les analystes affirment que le meilleur moyen de simplifier les transferts de fonds serait de « faire intervenir l'ordinateur dans la transaction ». On pourrait faire disparaître les documents si des terminaux – tous reliés aux ordinateurs des banques – étaient installés dans les magasins, les maisons et les bureaux. Il suffirait alors, pour effectuer une transaction, d'en introduire les données au moyen d'un téléphone ou d'un terminal à clavier.

On a fait beaucoup de publicité autour des cartes de crédit; pour bon nombre, elles annoncent la disparition du chèque; or, en se substituant aux espèces, les cartes de crédit ont eu pour effet, au contraire, de multiplier les chèques et les écritures. Dans les milieux

bancaires des États-Unis, on prévoit que 40 millions de personnes utiliseront les cartes de crédit bancaires pour effectuer $ 15 milliards d'achat annuellement. Au Canada, le système *Chargex* est de loin le plus développé, avec 3,2 millions de titulaires de cartes, et un volume d'affaires de $ 302 millions en 1971.

C'est dans un style familier que le passage ci-après, extrait d'un article récent[2], décrit la manière dont s'effectueront les échanges dans une vingtaine d'années.

> Au cours d'un voyage, Réal Lavoie a besoin d'argent liquide. Il passe à la banque et présente une carte d'identité, la seule carte dont il ait besoin, à une caissière, qui introduit la carte dans un terminal. Un voyant vert s'allume. La caissière presse quelques boutons et tend l'argent à Réal, qui signe un reçu.
>
> En rentrant chez lui, Réal n'a pas à se soucier du solde de son compte bancaire, car il a été payé la veille et son employeur a versé à sa banque le montant de son salaire au moyen du système de transfert par câble...
>
> Mais examinons plutôt la carte de Réal ... Elle comporte plusieurs éléments d'identification. Tout d'abord, le nom de la banque et le numéro d'identification (tous les deux en caractères lisibles et en code-machine); puis sa signature, sa photographie, et en plus un nombre à deux chiffres en caractères magnétiques. Le nombre à deux chiffres – produit, enregistré et stocké par l'ordinateur à la fin de la dernière opération bancaire effectuée par Réal – sert de mot de passe et donne accès au compte de Réal. Après chaque opération un nouveau nombre est produit, puis stocké; un faux ne pourrait pas présenter le bon numéro ...
>
> De temps à autre, Réal prend ses factures en langage-machine et se rend à un centre de paiement à deux pas de chez lui. Il appelle l'ordinateur central et insère sa carte d'identité dans une fente. La voix de contrôle le reconnaît. Il introduit successivement ses factures et la voix répète les instructions jusqu'à ce que la dernière facture ait été traitée.

Le mode de paiement des factures connaîtra sans doute une évolution graduelle, et il est possible qu'un jour on en utilise plusieurs simultanément. Cependant, quels qu'ils soient, ces modes de paiement, dans tous les cas, devront mettre complètement à profit la rapidité et l'immense capacité de mémoire des ordinateurs modernes. On peut prévoir que d'autres établissements, par

exemple les grands magasins, établiront des systèmes de données financières analogues.

Une utilisation croissante des ordinateurs par les banques peut entraîner des difficultés de toutes sortes. D'abord, les risques d'inexactitude dans les données seront plus élevés si un grand nombre de caissiers et d'employés de magasins ont la possibilité d'alimenter directement l'ordinateur central à partir de terminaux. Des entrées erronées dans les relevés de compte des clients se répercuteront sur leurs cotes de solvabilité. En outre, si les banques recourent davantage aux télécommunications, les membres de leurs personnels seront plus nombreux à avoir accès aux informations confidentielles par les terminaux ; il pourrait être alors plus difficile d'empêcher les fuites.

Toutefois les entreprises bancaires font face non seulement à la concurrence d'autres banques mais à celle d'établissements voisins, c'est-à-dire les compagnies de gestion et les caisses populaires. Dans un secteur d'activité de faible concurrence sur le plan tarifaire, on attache une importance extrême à la qualité du service. Par conséquent, une banque dont les méthodes de sécurité seraient insuffisamment strictes ou qui manquerait de rigueur dans le traitement des données serait tôt compromise sur le plan de la concurrence. Ce fait assure donc une certaine protection au consommateur. On peut aussi avancer, et il ne manquera pas de gens pour le faire, que l'amélioration des contrôles et la centralisation découlant de l'automatisation des tâches contribueront à une sécurité plus grande et à une précision accrue.

Malgré cela, n'allons pas croire que la sécurité dans les banques canadiennes est tellement plus grande que dans les banques de Grande-Bretagne où l'on peut se renseigner, nous l'avons déjà dit, pour $ 15,75 sur le solde des comptes personnels. Comme les banques devront accumuler des quantités d'informations personnelles toujours plus grandes, et qu'un système intégré de fiches financières personnelles se constituera probablement, il importe sans cesse davantage pour le public et pour les organisations jouissant de certains privilèges que les règles concernant l'utilisation des informations soient clairement définies et divulguées.

2. Les banques d'information médicale [3]

Selon une croyance des plus générales touchant la médecine, les rapports entre le médecin et le malade sont confidentiels et exempts de toute ingérence de tiers. Il s'agit là d'une conviction profonde ; le malade a une telle confiance en son médecin qu'il ne craint pas de lui dévoiler les détails les plus intimes de sa vie. Ainsi, il est plus facile pour le médecin de dispenser de bons soins avec chaleur et humanité.

Toutefois, une évolution s'est amorcée dans trois directions et pourrait fort bien transformer du tout au tout ces rapports. Premièrement, la médecine tend à devenir un travail d'équipe. Deuxièmement, elle a de plus en plus recours aux systèmes d'information. Troisièmement, le rôle social de la profession évolue. Les deux premiers phénomènes rendent difficile pour le particulier de préserver le caractère confidentiel des informations sur son état de santé.

La médecine d'équipe donne au malade la possibilité de se faire soigner par des spécialistes de toutes sortes. Quant au médecin, il en sera plus efficace, et pourra plus facilement se spécialiser. Par contre, les relations avec les clients perdent leur caractère particulier, le malade étant « partagé » entre les différents membres d'une équipe comprenant des médecins et un personnel paramédical. Certains dénoncent dans cette fragmentation une déshumanisation de la médecine. Pour les apaiser, divers hôpitaux des États-Unis ont recours à un « ombudsman » des malades.

La mise au point de systèmes d'information médicale répond à deux grands soucis : assurer de meilleures informations comptables et administratives ; fournir au personnel médical des informations de qualité supérieure et aux malades, par voie de conséquence, des traitements mieux adaptés. En fait on ne peut séparer complètement ces deux objectifs. Les provinces se servent des informations médicales contenues dans leurs fichiers automatisés à des fins qui ne sont pas toujours comptables, et que l'on peut répartir entre trois catégories :

- contrôler la nature des soins médicaux dispensés en demandant aux malades de vérifier si les imputations portées sur les comptes correspondent aux soins effectivement reçus ;
- effectuer des travaux de recherche sur les maladies

épidémiques et sur le recours aux soins médicaux par la population ;
- faciliter l'application de la loi.

Au Manitoba, on consulte les dossiers médicaux pour déterminer l'admissibilité au permis de conduire. Techniquement, il est possible de mettre en regard données médicales et informations détenues par d'autres services de l'État pour vérifier si on satisfait aux exigences et restrictions de la loi. Ainsi, ceux qui demandent des prestations ou d'autres formes d'assistance sociale invoquent souvent des raisons de santé.

Dans certaines provinces, les dossiers médicaux ont permis aussi d'estimer les revenus des médecins. D'ailleurs, les communications à la presse sur ce sujet ont suscité chez les médecins des plaintes d'intrusions dans leur vie privée.

Quelques systèmes de recherche documentaire à usages multiples pour le classement des informations médicales ont été mis sur pied, notamment le système des *Professional and Patient Activity Studies* (P.A.S.), de l'Université du Michigan, qui dispense ses services à un tiers environ des hôpitaux canadiens (tous les hôpitaux de l'Alberta sont obligés de l'utiliser) et indique les méthodes de traitement utilisées dans chaque cas. Plus récemment, l'*Hospital Medical Records Institute* s'est établi en Ontario, où il effectue des recherches statistiques et analytiques du même genre. Au Canada, 15 p. 100 des hôpitaux, approximativement, font appel à ses services.

Dans un certain nombre de centres médicaux l'ordinateur sert au diagnostic. Un hôpital écossais a fait l'expérience d'un système informatique recueillant du malade tous les renseignements nécessaires à son admission. Ceux-ci se sont révélés aussi exacts que s'ils avaient été obtenus par la méthode classique. De plus, 50 p. 100 des malades préféraient le dialogue avec l'ordinateur à l'entretien avec un médecin.

Le ministère de la Santé nationale et du Bien-être social tient à jour des informations médicales sur les aveugles, les infirmes, les sujets en rééducation, les autochtones de certaines régions, les personnes atteintes de maladies chroniques ou contagieuses, dont les maladies vénériennes et la tuberculose. Il se propose de créer un réseau de fichiers automatiques pour les 35 000 habitants des Territoires du Nord-Ouest ; ainsi les bureaux régionaux de la Santé seraient reliés au service central d'Ottawa par télécommunication. Les fichiers renfermeraient des informations sur l'état de santé de

chacun, sur les médecins, les installations, et sur les cas d'alcoolisme ou de toxicomanie. C'est le projet le plus important à l'étude, au Canada, dans le secteur de l'information médicale.

La centralisation et l'automatisation des fichiers médicaux posent certains problèmes qu'on a tendance à rattacher globalement à la vie privée ; il y en a de manifestes, par exemple les risques d'erreurs et d'utilisation des renseignements par des tiers, à l'insu du médecin et du malade, ou avec l'assentiment du médecin seulement.

Des erreurs peuvent se produire dès l'introduction des données. Nous avons fait état plus haut des nombreuses erreurs découvertes par une compagnie d'assurance sur la vie au cours de l'automatisation de ses fichiers. Mais cette compagnie n'a pas été la seule à connaître pareille situation ; en règle générale, il faut des précautions particulières, dès l'introduction des données. Et même si la transcription est sans faute, il subsiste des possibilités d'erreur soit celles de diagnostics inexacts et celles de rapports médicaux erronés.

S'il se produit des erreurs dans les diagnostics, c'est que ceux-ci, tout compte fait, procèdent par déduction des causes à partir des symptômes observés. De plus, les symptômes se prêtent souvent à plusieurs interprétations. Dans son diagnostic, le médecin ne fait pas que chercher les causes du mal, mais s'interroge sur les conséquences d'une erreur. Par exemple, s'agit-il de déterminer si telle personne peut conduire une automobile, ou si elle a droit à l'assistance sociale, le médecin sera prudent dans la rédaction du diagnostic. La situation est encore plus délicate quand le médecin constate une maladie vénérienne, ou encore des traces de coups sur un enfant ; la pensée de sa responsabilité civile ou de l'embarras chez le malade peut inciter à un compte rendu inexact des observations.

Une fois les données médicales stockées dans une banque d'information à accès multiples, le médecin et son malade perdent leurs prérogatives sur l'information. Nombre de gens pourront accéder à l'information et l'utiliser à l'insu de la personne qu'elle concerne. En effet, il est possible de reproduire les dossiers à l'aide d'un matériel électronique ; alors on ne cherchera plus généralement à rendre compte de l'utilisation des données qui peuvent former la matière de nouvelles banques, une fois effectué le premier transfert.

Les problèmes auxquels se heurte le corps médical revêtent un caractère particulièrement critique en psychiatrie. Dans un mémoire présenté par le *Clarke Institute of Psychiatry*, on pouvait lire :

> La psychiatrie, par rapport aux autres disciplines médicales, pose une difficulté particulière : le dossier comprend des informations d'ordre familial, personnel, social et sexuel. Il est évident que des fuites en ces domaines ont plus de conséquences qui si elles avaient trait, par exemple, à un ulcère au duodénum.

Le droit d'accès des malades à leurs dossiers intéresse beaucoup le corps médical. Dans son mémoire au Groupe d'étude l'*Ontario Medical Association* résume la question en ces termes :

> Un médecin d'Ontario, fait passer à l'un de ses malades l'épreuve dite *Minnesota Personality Inventory* (M.M.P.I.). Une fois ce long questionnaire rempli, il l'enverra à un laboratoire de Californie, où il sera interprété à l'aide d'un ordinateur. Puis, le compte rendu arrive, indiquant, par exemple, que le malade accuse des tendances au suicide ou des prédispositions à la schizophrénie. Bon nombre estimeront que le sujet ne doit pas avoir accès au document. Et si l'on accordait ce droit, le malade pourrait-il voir les dossiers du médecin ou les données du centre qui aurait effectué l'analyse ? Et en pareil cas conviendrait-il qu'un centre de traitement communique ses résultats à d'autres que le médecin qui lui aurait fait parvenir le questionnaire à analyser ? Et qu'en serait-il si le malade, parfaitement sain d'esprit, mais classé comme schizophrène par erreur du laboratoire, eût été privé de l'accès à son dossier pour raison de santé mentale ?

Nombre d'établissements n'accordent aux malades l'accès à leurs dossiers que sur autorisation du médecin et sous réserve qu'il soit présent. Cette solution semble raisonnable, si le médecin et le malade s'entendent bien. Toutefois des conceptions différentes de l'exercice de la médecine imposeront d'autres pratiques.

Il n'est donc plus possible de tenir comme nécessairement préférable que le diagnostic ou le traitement recommandé figurent sur la fiche médicale. Avant que les données soient introduites dans le système d'information médicale, le médecin et le malade devraient savoir exactement comment et à quelles fins ces informations seront utilisées.

D'après certaines autorités du domaine thérapeutique, la question du caractère confidentiel et privé de l'information médicale sera bientôt dépassée. On peut avancer que la libre circulation de ce type de renseignements permettra aux planificateurs, aux chercheurs et aux praticiens de doter la société des services de santé les plus efficaces. Toutefois, pour préserver des

relations de confiance entre médecin et malade, il faut que la communication de données confidentielles se fasse avec le consentement du malade, dans la mesure du possible. Et si le public est contre la libre circulation des informations médicales sur les malades, les autorités devront en être conscientes. Il se pourrait alors que les inconvénients l'emportent de beaucoup sur les avantages. Des malades méfiants tairont certains faits au préjudice de tous.

1. La matière de la section traitant des banques d'information du secteur bancaire est extraite en très large partie de l'étude de H. S. Gellman au Groupe d'étude, et qui a pour titre *Electronic Banking Systems and Their Effects on Privacy.*

2. KRAMER, R. L. et LIVINGSTON, W. P., « Cashing in on a Checkless Society », *Harvard Business Review,* septembre-octobre 1967, p. 142.

3. Presque toute la matière de cette section est tirée de l'étude de J. I. Williams qui a pour titre *Privacy and Medical Record.* À noter que cette étude constitue le chapitre 7 de celle de John Carroll, intitulée *Procedures, Practices and Problems.*

Chapitre 6
Les enquêteurs

La mission des agences d'enquêtes est la collecte de renseignements qui ne seraient pas librement divulgués en raison du peu de confiance réciproque entre certains membres de la société. On conçoit donc que ces agences n'emploient pas les mêmes méthodes de collecte des informations que les statisticiens ou les cadres administratifs.

La police est habilitée par la loi à recueillir des informations, tandis que les agences de renseignements commerciaux et les autres agences d'enquêtes, tels les bureaux de détectives privés, doivent compter sur leur débrouillardise et leur pouvoir de persuasion pour obtenir les renseignements dont elles ont besoin. D'un côté, la police s'emploie à faire respecter la loi ; de l'autre, les agences mènent des enquêtes, sous le couvert d'entreprises commerciales, cherchant à savoir si des accords commerciaux ont été enfreints ou sont susceptibles de l'être par certains clients.

La mission du Groupe d'étude se limitait aux répercussions de l'informatique sur le respect de la vie privée. C'est pourquoi la question des méthodes utilisées par les agences d'enquêtes pour recueillir l'information (par opposition aux méthodes de traitement) a été effleurée seulement, en dépit de l'intérêt que le public lui porte depuis longtemps déjà.

1. La police

En matière de traitement de l'information policière, la création du Centre canadien d'information policière (C.P.I.C.), qui devrait être en pleine activité en 1975, est sans doute l'événement le plus marquant de ces dernières années. En 1975, le gouvernement fédéral aura consacré $ 36 millions à cet établissement, qui sera dirigé par la Gendarmerie royale du Canada à Ottawa; le Centre utilisera un ordinateur I.B.M. 360/65 (plus un ordinateur de secours) avec un grand nombre de dérouleurs de bande magnétique et d'unités de disques, de façon à permettre l'accès au fichier central à 250 corps policiers répartis dans tout le Canada. Au départ, quatre fichiers seront constitués (en français et en anglais) : vols de véhicules, vols de biens divers, mandats non exécutés, et casiers judiciaires. Parmi ces quatre fichiers, seul celui des casiers judiciaires, qui compte environ un million d'articles traités manuellement, contient des informations présentant un caractère privé, et, à ce point de vue, nous intéresse.

L'étude qui doit déterminer la nature des informations à consigner dans le casier judiciaire automatisé n'est pas encore terminée; y figureront probablement le nom, le numéro du casier judiciaire, le numéro de pénitencier, la catégorie des empreintes digitales, les données du cahier des infractions et écrous et les noms des complices.

Les corps policiers canadiens tiennent actuellement leurs propres fichiers à l'aide de systèmes manuels. Un bon nombre perdront de leur utilité ou disparaîtront quand le C.P.I.C. fonctionnera, puisque les différents corps de police auront accès au fichier central qui contiendra tous les casiers judiciaires. Les règles d'utilisation de ce fichier n'ont pas encore été définies.

L'ordinateur se trouvera à protéger les informations contenues dans le système en ne répondant qu'aux terminaux autorisés; de plus, le système comportera un relevé des utilisations des terminaux. Le codage des données échangées entre terminaux et ordinateur central ne se fera pas en raison du coût élevé de cette opération.

Des règles précises touchant la manipulation et la diffusion des informations sur les criminels seront sans doute définies et annoncées au moment de la mise en exploitation du C.P.I.C., comme cela s'est produit aux États-Unis pour le *System for the Electronic Analysis and Retrieval of Criminal Histories.*

Voici quelques-unes des pratiques actuelles en matière de casiers judiciaires :

- On n'ouvre pas de casier judiciaire, on ne prend pas les empreintes s'il s'agit de condamnations en référé ou de condamnations de mineurs, aux termes des lois provinciales.
- Les casiers judiciaires des criminels grâciés constituent un fichier distinct, dont l'accès est extrêmement limité en vertu de la Loi sur le casier judiciaire (*Criminal Records Act*).
- La question des empreintes digitales est déterminante. Quand un suspect est accusé d'une infraction majeure, puis acquitté, son dossier ne sera supprimé que s'il demande qu'on lui rende ses empreintes digitales.
- Les dossiers sont conservés jusqu'à la mort du criminel, ou jusqu'à ce qu'il ait atteint 70 ans s'il n'a pas eu de démêlé avec la justice au cours des cinq années précédentes.
- Les empreintes digitales prises par les forces armées n'entrent pas dans les fichiers de la police.

Il ne faudrait pas confondre fichiers de police et casiers judiciaires. La police, il est vrai, tient des dossiers sur des suspects sans casier judiciaire, et la mention d'une arrestation non suivie d'une condamnation peut avoir des conséquences fâcheuses. Toutefois, comme il n'est pas prévu que ces dossiers seront transférés à l'ordinateur du C.P.I.C., on peut espérer qu'ils resteront définitivement dans des fichiers locaux.

Il est très difficile de se renseigner sur les fichiers touchant à la sûreté nationale. Tout ce qu'on peut vérifier est qu'ils existent effectivement, qu'ils sont manuels et doivent être automatisés plus tard. Il s'agit d'informations extrêmement secrètes. Il serait déplorable que des fuites se produisent, en raison de l'utilisation de ces informations, de leur origine (qui est la plupart du temps le ouï-dire) et aussi parce que ces fichiers renferment sans doute des renseignements sur des citoyens innocents.

Au cours d'une visite à la police du Toronto métropolitain le Groupe d'étude a constaté que la plupart des fichiers sont manuels. Ils comportent diverses rubriques : répertoire central, plaintes et victimes, accidents, biens volés, voitures volées, arrestations et infractions mineures. Le répertoire central contient un million de fiches sur les personnes recherchées ou portées disparues, les criminels, les infractions mineures, les suspensions de jugement, les interdits de séjour, les mises en liberté surveillée, les libérations conditionnelles et les jeunes délinquants.

2. Les agences d'enquêtes commerciales

Nous avons déjà établi la distinction entre agences de renseignements commerciaux et agences d'enquêtes commerciales. Le travail des agences d'enquêtes porte sur les personnes plutôt que les compagnies. Elles mènent des investigations sur les proposants en assurance-vie, incendie ou automobile, sur les candidats à un emploi, sur les personnes cherchant à obtenir du crédit (prêt hypothécaire, carte de voyage, etc.) et sur les auteurs d'une réclamation d'assurance. Leurs principales sources d'information sont les voisins. Les enquêteurs sont particulièrement soucieux des points suivants : abus de l'alcool, conduite automobile imprudente ou par des jeunes, négligence dans l'entretien de la propriété, réunions tapageuses, disputes familiales, infirmités physiques ou mentales. Ils se renseignent aussi auprès de l'employeur, et, dans la moitié des cas, entrent en contact avec l'intéressé lui-même. Le *Retail Credit of Canada*, l'agence d'enquêtes commerciales la plus importante au Canada, a fourni, en 1971, 600 000 rapports sur des personnes ayant postulé un emploi.

Comme les agences de renseignements commerciaux, les agences d'enquêtes tiennent des fichiers manuels et œuvrent à l'échelon régional ; elles procèdent à des échanges d'information à l'échelle nationale ou internationale quand les circonstances l'exigent. Les enquêteurs n'ont pas de formation spéciale et le taux de rotation du personnel est généralement plus élevé que dans les agences de renseignements commerciaux. Le tarif est généralement de $ 5 l'enquête ou de $ 10 l'heure pour les investigations importantes.

Dans un mémoire au Groupe d'étude, la *Retail Credit of Canada Inc.*, succursale de la *Retail Credit Company of Atlanta* (Georgie), soulignait que les agences d'enquêtes tenaient à fournir des renseignements précis de façon à conserver leur réputation auprès des clients, et prenait la défense du type d'enquêtes menées par ces bureaux en ces termes :

> Les enquêtes qu'on nous commande ont pour point de départ une proposition ou une demande de la part du sujet de nos recherches. Personne n'avancerait que les compagnies d'assurance-vie ou d'assurance-automobile doivent établir des polices ou fixer les primes en se fondant sur des informations qui, du point de vue du souscripteur, peuvent être insuffisantes ou erronées.

Et l'auteur du mémoire poursuit :

> Pour que le particulier ait la possibilité de rectifier au besoin un rapport, il suffirait que l'utilisateur (c'est-à-dire le client de l'agence), s'il refuse en partie ou en totalité, sur la foi des renseignements fournis par l'agence, le service demandé, communique sur demande le nom et l'adresse de l'agence au particulier, de manière que ce dernier puisse discuter les données du rapport avec un représentant de l'agence.

Sur l'obligation pour les agences de dévoiler leurs sources d'information, les auteurs du mémoire énoncent ainsi leur position :

> ... obliger par une loi les agences d'enquêtes à dévoiler l'origine des informations d'ordre personnel qu'elles recueillent aurait pour effet de tarir leurs sources et, par voie de conséquence, menacerait leur existence à toutes. Pour le moins, il deviendrait difficile d'obtenir des informations défavorables qui fussent sûres ; les personnes interrogées donneraient des renseignements favorables mais sans valeur ou bien s'abstiendraient. Dans le cas de demandes en suspens, il serait difficile d'obtenir un nouvel examen des compagnies d'assurance-automobile ou d'assurance-vie, des organismes prêteurs ou des employeurs, puisque la préférence en quelque sorte, pour ce qui est de l'information, irait à ceux qui refusent de se prononcer véritablement.

On ne peut nier la justesse de certaines observations faites par les auteurs de ce mémoire. Toutefois, il paraît utopique de croire que les compagnies après avoir rejeté certaines demandes en s'appuyant sur les renseignements fournis par une agence d'enquêtes, indiqueraient à leurs clients les vraies raisons de leur refus. Aussi, dans le système actuel, des erreurs apparemment négligeables peuvent être cause d'un préjudice sérieux.

Étant donné l'importance, pour la plupart des gens, des décisions fondées sur les informations fournies par des agences d'enquêtes, il serait légitime d'obliger ces organismes à avertir les gens de l'ouverture d'un dossier sur leur compte, et aussi de leur laisser voir le dossier moyennant un déboursé minime. La source d'information est moins importante que l'information elle-même. Si le *Retail Credit of Canada* a vu juste, dévoiler l'origine des informations aurait pour effet de faire disparaître les sources fiables ; toutefois, il semble important, pour des raisons d'ordre

psychologique, et pour certaines autres raisons, que les individus aient la possibilité de prendre connaissance directement des informations consignées dans leur dossier, sans passer par un interprète.

Chapitre 7
Le numéro d'identification unique[1]

Il est une question bien débattue, soit celle de savoir s'il est souhaitable d'attribuer à chaque Canadien un numéro d'identification unique, complétant ou remplaçant le nom, l'adresse et les différents numéros servant à l'identification (assurance sociale, permis de conduire, compte de banque et passeport). Dans presque tous les secteurs de l'économie, le code numérique se répand malgré une résistance latente de la population. Même si rien ne pousse très nettement à l'adoption du système, il faut signaler que de nombreux pays étrangers l'utilisent déjà. De plus, comme les économies qu'il permettrait sont de plus en plus évidentes, on peut prévoir que des pressions s'exerceront en sa faveur. Déjà, l'Association canadienne de normalisation caresse le projet d'une carte d'identité de format normalisé en fonction de l'ordinateur, avec un espace libre pour le numéro d'assurance sociale au cas où il serait adopté pour identification[2]. Une proposition semblable par l'*American National Standards Insitute* a donné lieu à une enquête auprès du public par le *Department of Health, Education and Welfare.*

Les partisans du numéro d'identification unique se recrutent dans les secteurs public et privé. Une étude par l'*American Bankers Association* auprès de 250 organisations de toutes sortes, depuis les entreprises de carte de crédit jusqu'aux hôpitaux, a révélé

que la plupart étaient favorables au numéro d'identification unique. Il est vrai que le gouvernement des États-Unis a récemment réclamé des banques privilégiées américaines qu'elles inscrivent le numéro de sécurité sociale au dossier de leurs déposants, pour permettre à l'administration fiscale de trouver plus facilement les informations propres à l'intéresser. Plusieurs banques canadiennes et certaines agences de renseignements commerciaux ont manifesté de l'intérêt pour le numéro unique, de même qu'un comité spécial de l'*Ontario Medical Association.* Toutefois, le comité estimait qu'il fallait auparavant régler les questions de l'accès, de la diffusion et de la sécurité.

Les partisans du numéro unique font valoir les avantages qui résulteraient de son utilisation pour les citoyens[3]. Ainsi, en Allemagne, grâce à ce système, toute personne qui déménage n'a qu'à notifier sa nouvelle adresse à un seul organisme, et celui-ci se charge d'avertir les divers ministères et organismes intéressés. Les partisans affirment en outre que pareille efficacité dans les services se traduirait par une réduction des coûts pour le consommateur, mais n'avancent aucun chiffre à l'appui de cette affirmation.

Ni les partisans ni les adversaires du numéro d'identification unique n'appuient leurs thèses sur des arguments concrets et persuasifs. En fait, les objections sont plutôt viscérales et reposent essentiellement sur des craintes : perte de l'anonymat, déshumanisation et cataclysme éventuel.

Chez le public, la crainte de perdre l'anonymat intervient essentiellement dans les préoccupations au sujet de la vie privée. C'est pourquoi le principal avantage signalé par les partisans du numéro unique, soit l'aide qu'il apporterait dans le recoupement et le regroupement des informations, est en même temps une cause d'inquiétude. Beaucoup de gens craignent que la constitution de dossiers complets ne les prive petit à petit d'un moyen très efficace de combattre la bureaucratie : l'anonymat voulu.

Ils appréhendent aussi que les fonctionnaires oublient un peu que derrière les numéros il y a des personnes. Le souvenir de la numérotation des juifs par les nazis au cours des années 30, et pendant la seconde guerre mondiale, nourrit sûrement cette méfiance. D'après l'enquête menée par le ministère des Communications, 62 p. 100 des Canadiens craignent que l'ordinateur ne les réduise à des numéros.

Enfin le désastre redouté se ramènerait à l'utilisation de ce système par un régime autocratique et à une centralisation des dossiers personnels au service de l'oppression. À ces arguments, on

oppose que le manque de dossiers complets sur les citoyens n'a pas arrêté les autocrates par le passé.

Divers pays ont déjà adopté le système du numéro d'identification unique, soit la Suède (1947), Israël (1948), la Norvège (1964), la Finlande (1965) et le Danemark (1968). D'autres pays s'y préparent, notamment l'Argentine, les pays du Benelux, la République fédérale d'Allemagne, le Japon, la Suisse, l'Espagne, la Corée du Sud et l'Allemagne de l'Est.

Au Danemark, le système a été adopté sans opposition. Cependant, une fois mis en œuvre, il a fait l'objet de nombreuses critiques, notamment dans la presse. Avec ce système, disait-on, il sera sans doute plus facile de constituer des informations sur les citoyens à partir de « numéros-personnes » et d'en user à mauvais escient. Aux États-Unis, en 1970, on a proposé d'inclure dans le recensement le numéro de sécurité sociale, mais on a dû y renoncer à la suite d'une opposition très vive du Congrès et d'autres milieux.

Actuellement, au Canada, il n'existe pas de numéro d'identité d'application générale. Le numéro d'assurance sociale n'est obligatoire à l'échelle fédérale que pour le régime de retraite, l'assurance-chômage et l'impôt sur le revenu, et au Québec pour le régime provincial de retraite. Un répertoire des numéros d'assurance sociale est tenu à jour par la Commission d'assurance-chômage. Le fichier comporte 13,5 millions de numéros, ce qui englobe presque toute la population active, des écoliers et divers groupements. Pour l'instant, on envisage une mise à jour automatique des articles tenant compte des naissances, des mariages et des décès, et de tout changement d'état civil. Le numéro d'assurance sociale comprend neuf chiffres. Le premier indique la région ; le dernier sert à la vérification des numéros précédents. Les chiffres intermédiaires n'ont pas de signification. La Suède utilise un numéro formé de dix chiffres qui ont tous un sens. Les six premiers indiquent la date de naissance, les trois suivants la région, le dernier étant un chiffre de contrôle. Au Danemark, le numéro comporte également dix chiffres ; les six premiers indiquent la date de naissance ; les autres forment un numéro d'immatriculation. Lors de l'adoption au Canada du numéro d'assurance sociale, on s'est opposé à l'idée d'y inclure les données sur la date de naissance et le sexe de crainte que ce soit ouvrir la porte à la discrimination. La Commission d'assurance-chômage étudie des projets ayant pour objet la révision de la numérotation d'assurance sociale ; cela coïncide avec une extension de ce régime à un plus grand nombre sur la demande de quelques provinces.

Au Canada, actuellement, presque tout le monde peut donner

de huit à dix numéros distincts pour s'identifier, soit ceux des domaines suivants : assurance sociale, assurance-chômage, certificat de naissance, naturalisation, assurance-maladie, assurance-hospitalisation, adresse, numéro de téléphone, permis de conduire, compte de banque ou de société de gestion.

De plus, la plupart des Canadiens savent qu'une vingtaine de pièces numérotées pourraient servir à leur identification en divers milieux : passeport, permis (pêche, camping, navigation, stationnement, etc.), inscription à l'école secondaire ou à l'université, police d'assurance, bulletin de radiographie, dossiers médicaux, ordonnance, obligations, coffrets de sûreté, emprunts sur gage, carte de membre à un club, factures et reçus, etc. Il se pourrait bien qu'un Canadien dispose de 35 à 40 pièces numérotées, en moyenne, pour établir son identité.

Jusqu'à 1967, dans le Yukon et les Territoires du Nord-Quest, les Esquimaux s'identifiaient par des disques numérotés qu'ils portaient autour du cou. On comprend qu'ils aient rejeté le système et se soient donné des noms entre 1967 et 1971 à la place des numéros. Dans les fichiers contenant les numéros des disques de naguère, comme sur les registres où figurent les noms nouveaux, on ne trouve que les indications normalement notées à la naissance.

La gestion automatique des fichiers est beaucoup plus facile si chaque fiche porte un numéro codé ; les noms et adresses en clair sont des sources d'erreur dans les opérations logiques. Si, pour un être humain, il semble raisonnable d'affirmer que le dénommé M. R. Lajoie du 12 rue Prieur d'un certain fichier est très certainement le M. R. J. Lajoie du 12 avenue Prieur figurant ailleurs, l'ordinateur préfère s'en tenir au numéro 418-851-218.

Les numéros en code permettent d'éviter l'inconvénient de l'homonymie entre deux personnes ou plus. En outre, l'échange de données entre ordinateurs sera moins onéreux : le numéro d'identité comprend moins de chiffres que le total des chiffres et des lettres dans le nom et l'adresse en clair. Ainsi le numéro d'identité occupe moins d'espace dans la mémoire et les opérations de tri se font plus vite.

Par le numéro d'identité on peut relier plus facilement les fiches, mais tous les problèmes d'intégration n'en seront pas résolus pour autant. Dans bien des cas, le rapprochement par numéro d'identité de deux fichiers automatiques ne pourrait se faire sans l'intervention de l'homme parce que les structures des fichiers ne sont pas compatibles. Les opérations de traduction et de conversion nécessaires pour rendre compatibles deux fichiers automatiques séparés sont longues et coûteuses. Cependant, si le Canada adoptait

le numéro d'identification unique, les créateurs de systèmes accorderaient sans doute plus d'attention à la compatibilité des fichiers, de façon que la fusion de fichiers automatiques soit plus simple à l'avenir. L'Association canadienne de normalisation, s'engageant dans cette voie, a proposé une norme d'identification des personnes en vue d'échanges d'information entre ordinateurs.

Certains organismes provinciaux n'ont pas voulu adopter le numéro d'assurance sociale pour leurs fichiers. Pour le permis de conduire, le ministère des Transports et des Communications de l'Ontario, par exemple, a refusé de se servir du numéro d'assurance sociale, qui ne contiendrait pas assez d'informations. L'Ontario se sert de sa propre numérotation, qui comporte des informations sur le conducteur, notamment sa date de naissance.

Deux nouveux programmes de sécurité du revenu développeront, s'ils sont adoptés, l'usage du numéro d'assurance sociale. Avec le nouveau programme d'allocations familiales (Revenu familial garanti), les mères de famille désirant bénéficier de ce programme devront s'inscrire puisque les chèques seront établis à leur nom. Le projet de loi sur les allocations de vieillesse prévoit aussi l'utilisation du numéro d'assurance sociale. Dans les deux cas, on déterminera les allocations en fonction du revenu déclaré, qu'on ferait confirmer par le ministère du Revenu national.

Il est possible que l'usage impose peu à peu un seul numéro d'identité, par exemple celui de l'assurance sociale, aux utilisations de plus en plus nombreuses, et malgré ses limites, ou encore celui de la carte de crédit ou du compte de banque[4]. Cependant le principe du numéro unique ne doit pas être retenu sans avoir fait l'objet d'un débat public et d'une étude approfondie de ses incidences.

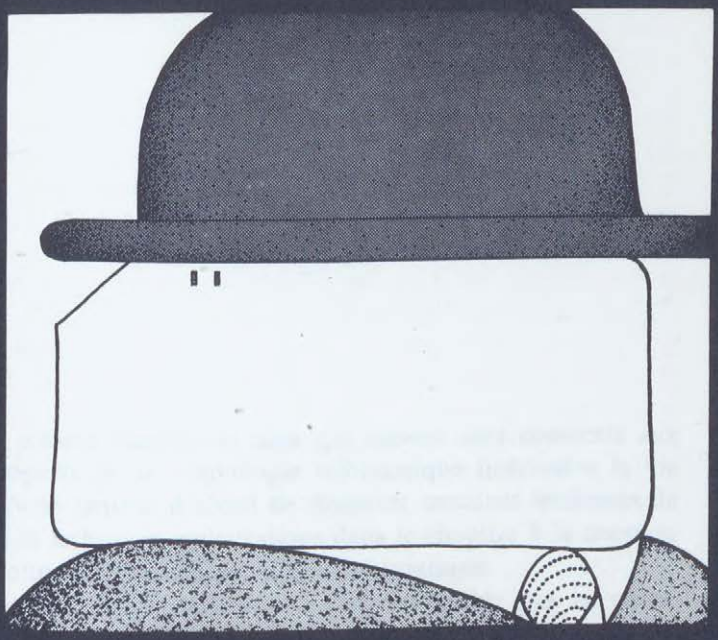
1. Ce chapitre s'inspire largement des études effectuées pour nous par H. S. Gellman et C. Kirsh et qui ont pour titre *Statistical Data Banks and Their Effects on Privacy*, d'une part, et *Profile of Personally Identifiable Records in Canada*, d'autre part.

2. Projet de normes de l'A.C.N. Z243.9 « Identification des individus permettant l'échange d'informations entre ordinateurs », 6e ébauche, 11 février 1962.

3. *PERSONNENKENWZEICNEN*, fascicule (en langue allemande) publié par le ministère fédéral de l'Intérieur, Bonn, République fédérale d'Allemagne, juin 1971. Ce texte avait pour objet d'exposer la position du gouvernement relativement à l'identification numérique des individus.

4. Les banques privilégiées américaines sont tenues par la loi d'identifier tous les comptes personnels à l'aide du numéro de sécurité sociale pour faciliter l'identification des individus en cas de fraude fiscale.

Troisième partie



Incidences de la technologie informatique

Chapitre 8
Perspectives d'avenir[1]

Le présent chapitre et ceux qui suivent sont consacrés aux divers aspects de la technologie informatique intéressant la vie privée. Nous tentons d'abord de discerner certaines tendances de l'évolution technique, puis traitons dans le chapitre 9 la question fort débattue de la sécurité en milieu informatique.

L'ordinateur, répétons-le, est bien incapable par lui-même d'immixtion dans la vie privée. Mais, il en multiplie les occasions en facilitant le stockage et l'extraction rapide d'un très grand nombre de données et leur diffusion presque instantanée indépendamment des distances; en favorisant la centralisation des informations; en rendant possibles la compilation et l'analyse de tableaux statistiques considérables. Bien que la technologie informatique n'ait pas atteint son plein développement, déjà les ordinateurs sont capables de trier et d'interclasser des fichiers considérables pour constituer des dossiers uniques à partir de sources disparates.

L'homme a déjà tendance à confondre information et sagesse, si bien que certains amassent de la documentation comme si elle était une fin en soi. Or, l'ordinateur vient renforcer cette tendance. Dans la mesure où leurs décisions se fondent sur des informations que fournissent les systèmes automatisés, les dirigeants auront

peut-être tendance à exagérer l'importance des données quantitatives. Dans son rapport final, publié en 1972, le groupe dit *Program on Technology and Society*, de l'Université Harvard, signalait ce qui suit :

> « D'une façon générale, les résultats des travaux de simulation sur ordinateur et d'analyse organique sont présentés sous une forme quantitative ; celle-ci crée parfois une impression magique de rigueur et d'infaillibilité que ne justifient ni la sécheresse des données ni la validité des hypothèses sur lesquelles elles sont fondées. »

L'aptitude des ordinateurs à passer au crible d'énormes quantités de données et à dégager des rapports non apparents entre les faits a été exagérée, compte tenu de l'état actuel de la technologie. Les grands fichiers exigent bien souvent plus de cent bobines de ruban magnétique pour le stockage ; comme il faut sept minutes pour lire un ruban il est évident que l'exploration de grands fichiers est à la fois longue et coûteuse. En fait, une reprogrammation considérable et onéreuse est souvent nécessaire pour de nouvelles explorations. Les progrès de la technologie permettront toutefois de réduire rapidement le coût et la difficulté de telles explorations.

Il n'en est pas moins manifeste que les ordinateurs peuvent aussi servir à la protection de la vie privée. On peut aisément programmer des systèmes automatisés pour tenir un registre des emplois d'un fichier ; il est en outre relativement simple de fournir des feuilles de sortie de fichiers si quelqu'un d'autorisé désire les examiner. De plus, comme l'automatisation mène souvent à la centralisation des fichiers, il est plus facile d'assurer l'exactitude des données et leur caractère confidentiel.

1. État actuel de la technique

On peut établir un parallèle entre l'industrie automobile du début des années 20 et le secteur informatique tel qu'il est aujourd'hui. Les principaux effets de l'automobile – développement routier et sidérurgique – étaient prévisibles ; les répercussions indirectes de grande portée, soit la croissance des villes, la mégalopolis et la pollution ne furent pas prévues généralement, du moins pas par ceux qui auraient pu adopter les mesures nécessaires.

Quant à l'ordinateur, c'est maintenant un cliché de dire que nous avons à peine entamé ses possibilités d'application. Dans le présent chapitre, nous allons essayer d'examiner les incidences immédiates de l'ordinateur. On ne peut malheureusement que

spéculer sur les effets à long terme. Ainsi, au *Stanford Research Institute*, Engelbard[2] étudie comment accroître les possibilités intellectuelles de l'homme. Ses travaux, qui bénéficient d'une aide importante d'organismes américains de recherche, visent à élaborer une nouvelle ambiance de travail en mettant l'accent sur le travail d'équipe. Dans ce cadre, l'ordinateur n'est qu'un outil, essentiel cependant, de collecte de données pertinentes, d'analyse sous divers angles et de communication entre collaborateurs.

Les répercussions des travaux d'Engelbard sont difficiles à prévoir ; cependant, on peut se représenter les effets à court terme de certains perfectionnements techniques sur la vie privée[3]. Il semble bien, par exemple, que d'ici dix à vingt ans le gros des informations sera enregistré sur support informatique. Le principal obstacle est le coût élevé des appareils de stockage à accès sélectif et de la transcription des renseignements sur support informatique. Cependant, le coût des mémoires à accès sélectif diminue rapidement ; quant à l'adoption des techniques de composition automatique et des équipements automatisés qui permettent la mise au point de textes (tels ceux qui ont servi pour le présent rapport), elle signifie qu'une grande partie de l'information originale se présentera d'abord sous forme numérique, ce qui n'exigera aucune conversion. De plus, l'emploi de techniques optiques de balayage a beaucoup fait pour réduire le coût de conversion de l'information imprimée en information sur support informatique.

L'ordinateur s'est perfectionné à un rythme remarquable. C'est l'Allemagne qui, en 1941, fabriqua le premier calculateur numérique fonctionnel. Deux autres événements ont fait époque : la construction, en 1944, de l'ordinateur Harvard Mark I qui mettait 4,5 secondes pour faire une multiplication à l'aide de relais électromécaniques ; la mise au point, en 1946, de l'ENIAC, 2 000 fois plus rapide que le Mark I. L'ordinateur le plus rapide à l'heure actuelle fonctionne à des vitesses de 500 millions de fois supérieures à celle du Mark I. Depuis 1952, année où commença à se répandre l'utilisation commerciale de l'ordinateur, le coût d'exécution moyen d'une instruction a été réduit au dix-millième environ.

La vitesse et le coût des ordinateurs continueront d'évoluer favorablement, mais un certain ralentissement de ces progrès est à prévoir. Les laboratoires travaillent actuellement à de nouvelles techniques (telles que le traitement optique, les appareils exploitant l'effet dit de Josephson, le traitement associatif) qui laissent entrevoir un décuplement des vitesses de traitement en dix ans ; l'emploi généralisé des circuits intégrés pour la logique et pour la mémoire à accès rapide entraînerait une réduction des prix

pouvant atteindre 99 p. 100 pendant la même période. Toutefois, les possibilités techniques ne connaissent pas nécessairement une mise en œuvre commerciale immédiate. Les considérations économiques et sociales interviennent également.

Jusqu'ici les principaux fabricants d'ordinateurs ont pu vendre leur équipement à dix fois environ le coût de fabrication. Cette forte marge a permis un taux de croissance élevé et soutenu, facilitant les investissements nécessaires à l'expansion, aux travaux de recherche et à la mise en marché. Reste à savoir si l'on pourra maintenir une telle marge au cours de la prochaine décennie. En admettant que le marché du matériel informatique reste concurrentiel, il semble inévitable que la marge bénéficiaire diminue à mesure que l'on se familiarisera avec la technologie.

L'investissement mondial en matériel, en programmerie et en perfectionnement du personnel dépasse maintenant les $ 100 milliards. Au Canada, l'équipement à lui seul absorbe plus de $ 1 milliard. Le taux de croissance annuel des investissements en matériel au Canada et aux États-Unis a fluctué entre 17 et 20 p. 100 en moyenne au cours des cinq dernières années. En 1980, les investissements canadiens à cet égard devraient dépasser de beaucoup les $ 4 milliards.

Le rythme rapide de l'évolution technologique tient pour une large part à l'appui considérable du gouvernement américain, accordé surtout par l'intermédiaire de l'*Atomic Energy Commission* et du ministère de la Défense nationale. Dans les années 70, ce sera plutôt une action gouvernementale conçue pour les entreprises commerciales et les citoyens qui offrira les stimulants nécessaires au progrès technologique.

La réduction des coûts découlerait surtout d'économies au chapitre du stockage. D'ici quelques années, les grandes organisations se procureront sans doute des systèmes de mémoire à accès direct d'une capacité de 10^{12} bits ou plus contre 10^{9} actuellement, et réduiront ainsi au centième ou à moins encore les frais de stockage. Étant donné le rôle essentiel de la mémoire dans les systèmes informatiques, toute amélioration en ce domaine se répercutera sur la nature et le rendement des banques d'information.

Grâce à une réduction considérable du coût des circuits électroniques, on peut désormais doter les petits ordinateurs de certains perfectionnements qui étaient réservés aux appareils de grande taille. Certains miniordinateurs offrent compilateurs Fortran, adaptabilité au matériel complémentaire et utilisation en temps partagé. À la nouvelle souplesse des miniordinateurs

s'ajoutent les fortes économies d'échelle propres aux superordinateurs, en particulier dans les applications intensives ou celles qui exigent beaucoup de manipulations et de très grands fichiers. Mentionnons aussi les immenses systèmes de stockage de données, fort coûteux à l'achat mais où le coût unitaire de l'enregistrement est très bas. Pour une mémoire à accès relativement rapide, on pourra disposer de disques et de tambours de plus en plus grands. Pour une mémoire de masse à accès plus lent, des dérouleurs de bandes de haute densité d'enregistrement de même que les mémoires holographiques et au laser, laissent entrevoir pour les systèmes à bande ordinaire une réduction du coût de stockage de quelque 0,01 cent par bit à quelque 0,00001 cent par bit vers 1975.

Les ordinateurs géants, pour être rentables, exigeront un taux d'utilisation élevé; il faudra donc, pour de nombreuses applications, qu'ils puissent recevoir des téléentrées à un coût raisonnable. Au Canada, le trafic téléinformatique entre déjà pour 6 p. 100 environ du revenu total des télécommunications; il s'accroît deux fois plus vite que la transmission à fréquence vocale. Le facteur distance dans les tarifs de transmission numérique diminuera sensiblement à mesure que le coût des installations pour le service interurbain décroîtra proportionnellement dans les dépenses de télécommunication. Malgré les changements que connaîtront sans doute les tarifications, et la difficulté consécutive des comparaisons, il est probable que vers 1980 les taux de télétransmission de données se situeront entre le tiers et le neuvième de ce qu'ils sont aujourd'hui. À mesure que les coûts de télétransmission numérique diminueront et que la qualité du service s'améliorera, la centralisation des bases de données informatisées sera de plus en plus rentable.

Vers la fin des années 70, l'emploi des ordinateurs dans les familles commencera à susciter une demande, mais les services de ce type ne devraient pas se répandre durant la décennie. Les premiers services aux foyers comporteront probablement des téléphones à clavier et la réponse vocale par ordinateur. Il existe déjà quelques systèmes rudimentaires de ce genre.

De nouveaux progrès dans les techniques de temps partagé de même que des télécommunications numériques et des terminaux moins onéreux vont permettre de contrer la tendance à la centralisation des pouvoirs, qui semble découler de la centralisation des systèmes d'information. Car, si des économies d'échelle peuvent en toute vraisemblance mener à la centralisation du stockage de l'information, les moyens technologiques liés au temps partagé et

aux télécommunications numériques permettent un accès à l'information hautement décentralisé. Les conflits de pouvoir reliés au droit d'accès à l'information vont donc très probablement se multiplier à mesure que se développeront d'importantes sources d'information centralisées. Les confrontations récentes à propos de l'accès aux bibliothèques universitaires préfigurent la nouvelle lutte pour l'information.

Selon un lieu commun des revues spécialisées, la technologie du matériel informatique a connu un développement beaucoup plus poussé que la technologie de la programmerie ou des techniques de programmation. On cite souvent en exemple le piètre rendement de nombreux systèmes de gestion automatisée, surfaits et chers. Un slogan qui cerne davantage le problème qualifie les années 70 de « décennie de l'utilisateur (d'ordinateurs) ».

Les débuts de l'industrie informatique virent des constructeurs relativement bien qualifiés sur le plan technique vendre l'équipement à une clientèle fascinée mais, somme toute, ignorante. Le fabricant réussissant le mieux était celui qui offrait un service complet : il déchargeait ses clients des nombreuses décisions dont ces derniers se sentaient incapables. Il n'est pas étonnant, dans les circonstances, qu'il y ait eu surabondance de systèmes incapables de satisfaire à la fois au calendrier de mise en application, aux prévisions financières, voire aux spécifications techniques. Il surgissait même des difficultés dans des systèmes relativement simples où l'on connaissait les paramètres de spécifications – pour les feuilles de paie par exemple. Dans une telle ambiance, les systèmes de gestion automatisée, censés fournir aux cadres supérieurs et moyens l'information dont ils avaient besoin, avaient peu de chance de succès. On manquait surtout d'analystes capables de comprendre les problèmes des clients, et il eût fallu des utilisateurs au fait des possibilités et des limites des ordinateurs. Des progrès sensibles ayant été réalisés sous ces deux rapports, l'utilisateur aurait maintenant le pas sur le constructeur.

Dans un article publié en 1970, un expert de A. D. Little Inc.[4] déclarait en être venu à la conclusion, avec ses associés, que de là à 1975, aucun développement fondamental de la programmerie n'aurait lieu et que d'ailleurs aucun ne serait nécessaire. Il ajoutait cependant qu'il restait encore de sérieux problèmes quant au meilleur usage possible de la programmerie existante. Il est certain que les langages machine s'amélioreront et qu'apparaîtront de bien meilleurs systèmes de gestion des fichiers centraux. On mettra également à profit de nombreux systèmes d'application à partir de la technologie existante. En outre, étant donné que le coût de la

programmerie représente une part de plus en plus importante des dépenses, alors que celui du matériel diminue, il est possible que l'on s'intéresse moins au développement optimal du matériel et davantage à un meilleur emploi du programmeur et de l'analyste. Toutefois, ces tendances mises à part, ce qu'on prévoit d'abord en programmerie, c'est la participation de l'ordinateur à l'élaboration des programmes. Ces progrès influeront beaucoup sur les conditions financières du développement de la programmerie dans la deuxième moitié de la décennie.

2. En résumé

Nous fondant sur ce qui précède, nous pouvons tirer quelques conclusions générales sur les tendances qui se dessinent dans le domaine de la technologie de l'informatique.

1. Grâce à de nouvelles réductions dans le coût du matériel informatique, de nombreuses applications qui ne sont pas économiques ou ne le sont que marginalement, vont devenir viables, notamment les systèmes bancaires et de crédit en liaison directe et de nouveaux systèmes de santé et d'enseignement.
2. On verra apparaître des ordinateurs ultra-rapides reliés à de très grands systèmes de mémoire à accès direct et dotés d'une programmerie très perfectionnée pour la gestion des données ; ainsi il sera rentable de chercher les données dans diverses banques d'information de grande taille pour les regrouper en de nouvelles catégories. Les gouvernements comme les entreprises vont en faire un usage constant afin d'élaborer des modèles de simulation pour l'examen des choix s'offrant à eux. Il va sans dire que ce perfectionnement va entraîner un besoin accru d'informations détaillées et exactes de tout genre, dont celles de caractère personnel sur les individus.
3. À l'heure actuelle, d'importantes économies d'échelle peuvent être réalisées dans l'exploitation des grandes banques d'information. D'autre part, les immobilisations considérables qu'exigent les grandes mémoires pousseront à économiser en centralisant les fichiers numériques. Toutes les fiches sur une personne (médicales, judiciaires, fiscales, professionnelles) ne seront pas forcément fondues en un énorme dossier

numérique, mais elles pourraient être groupées dans la même pièce pour faciliter l'échange des données.

4. Un très haut pourcentage des systèmes informatiques de moyenne et de grande taille seront reliés à des points éloignés par télécommunication. Cela peut tout aussi bien accélérer le mouvement vers la centralisation que vers la décentralisation, entraînant dans un cas comme dans l'autre d'importantes répercussions sur les structures politiques et sur la vie privée.

Jusqu'à présent les effets des ordinateurs sur la vie privée n'ont pas été que positifs. Si les avantages sont manifestes, on constate aussi que les inexactitudes abondent et que l'ordinateur contribue à la dépersonnalisation et à une centralisation accrue du pouvoir. Dans les jeunes années de l'informatique, peu de gens s'interrogeaient sur ses incidences éventuelles au plan humain, ou connaissaient assez bien l'ordinateur pour le plier, comme un outil, aux fonctions désirées et prévenir les effets indirects non voulus. Depuis lors, les connaissances et la conscience se sont accrues, et pourvu que la volonté y soit, l'ordinateur peut servir à décentraliser l'information et le pouvoir et à défendre la vie personnelle et l'individualité dans une société de plus en plus complexe. L'ordinateur peut le faire en mettant à la disposition de tous des services que seuls les riches et les puissants peuvent s'offrir aujourd'hui. Par contre, l'usage de l'ordinateur pourrait, délibérément ou non, donner raison à l'auteur de « 1984 ».

1. La matière du présent chapitre est tirée de l'étude effectuée pour le Groupe d'étude sur l'ordinateur et la vie privée ainsi que pour le Groupe d'étude sur la téléinformatique au Canada, intitulée *Technological Review of Computer Communications*.

2. Voir LINDGREN, Nilo, « Toward the Decentralized Intellectual Workshop », *Innovation*, n° 24, septembre 1971, pp. 50 à 60.

3. Voir NIBLETT, G. B. F. *Digital Information the Privacy Problem*, O.C.D.E. Rapport n° SP(71)4, Paris, mars 1971, pp. 4 à 8.

4. WITHINGTON, Frederick G. « Trends in MIS Technology », Datamation, vol. 16, n° 2, février 1970, p. 108.

Chapitre 9
La sécurité dans les banques d'information automatisées[1]

Si l'on veut contrôler la diffusion des renseignements personnels que renferment les banques d'information, il faut veiller à ce que les données soient stockées et traitées en toute sécurité. Toute la question de la sécurité mécanographique a d'ailleurs été fort débattue ces dernières années, non tant sous le rapport de la vie privée que sous celui de la sécurité de l'industrie, domaine où les propriétaires d'ordinateurs sont exposés au sabotage par des révolutionnaires ou des employés, ainsi qu'à l'espionnage industriel. Les gouvernements et en particulier les militaires connaissent depuis longtemps ce problème de sauvegarde des données confidentielles.

De pittoresques anecdotes ont cours à ce sujet, dont celle qui suit, probablement inventée de toutes pièces. Le programmeur d'une grande banque avait commandé à l'ordinateur d'arrondir les états financiers et d'en affecter les fractions de cent à un compte spécial, en l'occurrence le sien ; il se serait enrichi de la sorte. D'autre part, il est techniquement vrai qu'un saboteur peut, avec un simple aimant, mettre hors d'usage des rubans magnétiques contenant de précieuses données ; mais il ne pourrait passer plus

d'une centaine de rubans en une soirée, le procédé n'étant pas rapide. Il est arrivé aussi, dans une entreprise soumissionnant la programmation et les calculs, qu'un employé, grâce à sa connaissance des mots clés, dérobe un programme à l'ordinateur du principal concurrent en composant le numéro de l'appareil et en posant les questions qu'il fallait. On le surprit par hasard. Le programme étant imprimé au même instant dans la principale salle des machines, quelqu'un se demanda qui pouvait bien l'utiliser.

En définitive, la protection des données dépend d'un ensemble de contrôles. Celui-ci d'ailleurs n'est jamais absolument efficace : le degré de protection est fonction de ce qu'il en coûtera à l'intrus pour déjouer les dispositifs de sûreté, relativement à ce que lui vaudront les données. D'autre part, pour qui veut assurer la protection des données, le coût de la mise au point et de l'application des contrôles doit être faible relativement aux pertes qu'entraînerait une atteinte à la sécurité. Il convient de citer ici le mémoire présenté par l'Association du téléphone du Canada :

> « Jamais les réseaux informatiques ni les systèmes d'ordinateurs et de banques d'information ne seront complètement sûrs. Quelle que soit la qualité du chiffrage ou des techniques de protection, les mesures de sécurité pourront être violées si le butin en vaut la peine »

Dans le cas des banques d'information militaire, les données ont une importance telle que l'on n'épargne pratiquement rien pour en assurer la protection. Il est clair, toutefois, que ces systèmes constituent des exceptions. Aussi le présent chapitre traite-t-il plutôt des banques de données commerciales ou publiques où les dépenses de protection sont encore à une échelle bien plus modeste.

Dans le domaine de la protection des systèmes automatisés, deux attitudes s'opposent. Généralement, dans les installations névralgiques, on a tendance à protéger la totalité du système, n'admettant près de l'équipement que des personnes munies de l'autorisation sécuritaire ; de plus on a recours à un code lorsque la transmission des données se fait en dehors de la zone protégée. À l'opposé, nous avons l'ordinateur en temps partagé et à nombreux terminaux (souvent accessibles par téléphone à cadran), et un utilisateur qui peut déléguer son droit d'accès aux fichiers ; on y applique des mesures de sécurité telles que le mot de passe, mais elles ne sont pas obligatoires. Dans les deux cas on se soustrait au problème que peut poser la coexistence dans un même système de données délicates et de données ordinaires.

Avec l'avènement de grands ordinateurs exploités en temps partagé, il est de plus en plus avantageux de combiner dans un

même ordinateur des systèmes dont les conditions de sécurité varient selon la nature des travaux. Alors, il faut être en mesure de fournir une certaine protection, sans toutefois isoler l'ordinateur de ses terminaux éloignés ni défendre aux utilisateurs de partager les données ou les programmes.

À propos des mesures de protection, on rappelle souvent le dicton voulant que la chaîne ne soit pas plus forte que le plus faible de ses maillons. Le problème de la sécurité suppose tout un train de mesures, car une protection partielle ne vaut guère mieux que l'absence totale de protection. La sécurité physique des installations, les tests d'intégrité et de loyauté du personnel sont tout aussi importants que les mesures de protection internes du système informatique.

Les éléments les plus importants de la protection des systèmes informatiques sont traités ci-après.

1. Les mots de passe

Les mots de passe ou les mots clés sont communément employés dans les systèmes informatiques à temps partagé ; ils ont un effet préventif sur les indiscrets. Il faut enregistrer ces mots de passe à deux endroits : chez l'utilisateur et dans le système. Dans les deux cas, ils risquent d'être divulgués. On a déjà suggéré l'emploi d'un mot clé ne devant servir qu'une fois et qui proviendrait d'une liste ; après chaque emploi l'utilisateur passerait au mot suivant pour le présenter à la machine ; ce moyen permettrait de déjouer l'interception des mots clés, de sorte que l'intrus n'aurait pas constamment accès au système. La méthode est toutefois peu répandue comme la plupart des utilisateurs estiment qu'il serait peu commode de tenir de ces listes.

Pour la plupart des systèmes informatiques, il est nécessaire que l'utilisateur ait un numéro d'autorisation ou de compte auquel on porte les frais de calcul. Ce numéro n'est guère utile que dans les cas de très faible précaution sécuritaire, puisqu'il est souvent imprimé pour les besoins comptables ou pour identifier les sorties de l'ordinateur. En outre, il est gênant de changer un numéro de compte qui aurait fait l'objet d'abus. Il faudrait que l'utilisateur puisse changer de mots clés aussi souvent qu'il le désire.

Les mots clés peuvent servir également à authentifier l'identité d'un utilisateur afin de lui donner accès au système ; il peut aussi authentifier l'autorisation donnant accès à un certain fichier. Le mot clé d'un fichier peut être inclus dans le tableau des droits d'accès à côté du numéro de compte de l'utilisateur ; il peut aussi

faire partie de l'étiquette stockée avec le fichier. Le mot clé du fichier est la deuxième ligne de défense contre les usurpations d'identité.

2. Le codage

L'emploi des tables d'écoute téléphonique, sorte d'indiscrétion électromagnétique, présente un risque lorsque les données sont transmises par des câbles en zone non protégée. De nombreux systèmes comportent le recours aux installations des sociétés exploitantes, qui connaissent bien ces problèmes. Il faut transformer, c'est-à-dire coder les données délicates à transmettre d'un point à un autre afin de les protéger. Les meilleures techniques de codage comprennent des clés de transformation aussi longues que les données elles-mêmes. La série de caractères qui composent la clé est déterminée par un numéro de départ, exactement de la même manière qu'une séquence de nombres pseudo-aléatoires. La séquence d'arrivée correspond au numéro de départ. Il est presque impossible de découvrir par le captage de la transmission le nombre de départ ou l'algorithme qui détermine la série.

Le déchiffrage du code exigerait un travail énorme. Il y a par exemple 10^{26} substitutions utilisables des vingt six lettres de l'alphabet. La valeur de protection d'un code dépend du degré de pénétration possible si le code est connu. Quand un système emploie nombre de clés et qu'on les change fréquemment, un travail de quelques heures par clé pourrait cependant dépasser au total les ressources de l'intrus.

Certains dispositifs, en usage depuis longtemps pour les messages diplomatiques, permettent de transformer un texte intelligible en un message codé ; la clé de la transformation est produite par le même dispositif (codage, décodage) installé sur des boutons ou des roues. Ce dispositif est en réalité un ordinateur spécialisé. L'opération pourrait se programmer sur miniordinateur, au besoin. Il faudrait alors que celui-ci soit protégé et placé sous la surveillance d'un responsable de la sécurité des systèmes. Le traitement des données serait effectué par l'ordinateur principal au centre du réseau et l'on n'aurait besoin des autres ordinateurs que dans les stations éloignées. Des dispositifs à coder et décoder se trouvent aujourd'hui dans le commerce.

On peut faire en sorte que ces dispositifs codent ou non la chaîne des entrées suivant des caractères spéciaux de contrôle dans la chaîne elle-même. Dans une fiche personnelle, par exemple, il se peut que les zones d'identification soient codées mais non les zones

numériques. Ainsi, le traitement des données statistiques pourrait se faire sans décodage alors que l'information reliant les valeurs numériques aux individus serait illisible à moins qu'on en connaisse le code.

3. Contrôle d'accès restreint

Il arrive souvent que l'on veuille limiter l'accès d'un fichier à une seule personne ou à un groupe restreint; parfois aussi on souhaite que certaines personnes aient accès à diverses parties seulement des données. Ainsi, dans un hôpital, les techniciens en radiographie n'ont accès qu'aux dossiers de leurs patients; d'autre part, le service de comptabilité, tout en ayant accès aux dossiers de tous les malades, peut se voir interdire les fiches qui contiennent le diagnostic médical; par contre, un investigateur devra peut-être avoir accès à toutes les zones sauf celles contenant le nom et l'adresse.

La plupart du temps, ceux qui ont accès à un fichier ont accès à toutes les zones de tous les dossiers. Avec un fichier manuel où l'on garde les dossiers dans des chemises, il est difficile de faire autrement. Dans un système informatique, toutefois, on peut limiter le droit d'accès à certains dossiers (ceux de certaines personnes seulement) ou à des domaines précis (données de facturation), ou encore à une combinaison de catégories. De même, on peut déterminer les privilèges de rectification des dossiers, le cas échéant; enfin, on peut restreindre les rectifications à la suppression, l'adjonction et la modification de données ou à la combinaison de ces trois opérations.

Les droits d'accès doivent être explicités dans tous les cas où des droits restreints existent; par exemple, lorsque le fichier est à accès limité ou lorsque la lecture est permise mais non les changements ou les suppressions. Il est possible de stocker avec les données, ou séparément, un tableau énumérant les utilisateurs autorisés et leurs droits d'accès. Quant à l'accès à ce tableau, il se limite strictement aux personnes autorisées à modifier le tableau, soit en général le propriétaire des données lui-même.

Souvent, c'est la programmerie (système de contrôle) qui en vérifie l'accès étant donné que dans la plupart des systèmes informatiques les opérations reliées aux fonctions de lecture et d'écriture sont déjà sous un contrôle central. La protection des données peut s'appliquer à différents niveaux du système d'exploitation. À cause de l'énorme complexité des systèmes modernes d'exploitation, il est difficile d'éviter entièrement que ne se créent, à

l'occasion, des « issues » qui servent aux transmissions non autorisées.

4. Livres de vérification

Tous les systèmes informatiques comportent des programmes de comptabilité, dont la tenue d'un livre pour tout ce qui touche aux imputations de frais pour services mécanographiques. Ces livres n'indiquent pas toujours les manipulations qui n'entraînent pas de frais. Comme la protection ne peut pas être absolue bien que les systèmes d'exploitation se soient énormément améliorés, les vérifications à rebours sont essentielles pour détecter les atteintes à la sécurité. Souvent l'interprétation du livre est difficile et très longue ; il convient donc d'en confier l'analyse au système informatique lui-même. Si l'analyse des cas suspects se fait instantanément, par exemple s'il y a emploi de mots clés inexacts ou efforts pour aller au-delà de la zone d'adresses assignée, un signal d'alarme peut se déclencher. Les mesures possibles à ce moment vont de l'expulsion de l'utilisateur à la fermeture de tous les fichiers en passant par la fermeture de la ligne de transmission. Le livre de vérification peut être conçu pour révéler toute espèce d'anomalie ; de toute façon il doit faire partie des moyens mis à la disposition de tout responsable de la sécurité d'un système informatique.

Les systèmes d'exploitation doivent comporter des livres de contrôle parfaitement à jour et être accessibles à des équipes indépendantes de vérificateurs de programmes ; ainsi on s'assurera que les contrôles nécessaires ont été faits, qu'ils n'ont pas été contournés. Enfin, il ne faut pas oublier que si l'accès au système d'exploitation n'est pas strictement réservé aux responsables de la sécurité, les dispositifs de vérification et les signaux d'alarme peuvent être désamorcés par un intrus.

5. Sécurité physique

L'usage voulant que les ordinateurs soient bien à la vue est en voie de passer. Pour la surveillance du cadre physique, il importe que le matériel soit installé dans des salles spéciales ; de plus l'accès à ces pièces exige un contrôle rigoureux. Il faut éviter non seulement la destruction de l'équipement mais aussi la divulgation des données en cours d'impression ou simplement exposées. Toute personne ayant accès aux pièces où se trouve l'équipement devrait s'identifier et justifier sa présence. Les modes d'identification par

plaques sont choses courantes. Tantôt l'accès est surveillé par un responsable de la sécurité et tantôt il est réglé pas des dispositifs que l'on ouvre à l'aide de plaques ou de verrous à combinaison. Dans de nombreuses organisations on exige que les visiteurs, comme les membres du personnel, portent un insigne les autorisant à pénétrer dans le centre de calcul. Malheureusement, dans bien des cas, on n'applique pas rigoureusement ce système ; on n'a alors qu'un semblant de protection.

Lorsqu'un élément du matériel est rattaché à distance à l'ordinateur central, le poste terminal est laissé souvent sans surveillance ou à peu près. Il s'ensuit que l'on manipule rarement des données vraiment délicates dans un système informatique doté de terminaux éloignés. Il est important que l'on puisse identifier les utilisateurs correctement de même que les terminaux, non seulement au début de la « conversation » mais par intervalles pendant un dialogue prolongé. Ce genre de vérification ne se produit que rarement sauf dans les systèmes militaires. Les terminaux à distance constituent, pour les intrus, les principales voies de pénétration.

Il est d'usage courant de détruire les données sur papier lorsqu'on n'en a plus besoin, mais on néglige souvent d'effacer celles qui se trouvent sur rubans ou dans les mémoires. Comme tout enregistrement efface le précédent, on a l'habitude de laisser sur les rubans comme dans la mémoire l'information enregistrée. Si les données sont délicates, l'utilisateur doit les supprimer par des chaînes de caractères dénués de sens pour ce qui est de la mémoire centrale. Quant aux rubans et aux disques, c'est plus difficile ; ils exigent plusieurs enregistrements de parasites pour que disparaisse l'information résiduelle. Certains experts en protection soutiennent que l'on ne peut jamais effacer complètement les données des rubans ou des disques magnétiques, quel que soit le nombre d'écritures ultérieures. Dans des conditions ordinaires, toutefois, la destruction des rubans comme elle se pratique chez les militaires serait superflue.

6. La sécurité et le personnel

Quiconque a accès à des données peut être source de fuites. Le moyen d'intrusion le plus direct est le contact avec un titulaire de poste de confiance. Aussi emploie-t-on divers moyens pour réduire les risques d'abus de confiance, dont les enquêtes sur l'intégrité et les peines en cas d'infraction. Avant tout, on doit réduire au minimum les occasions de fuites accidentelles en établissant des

méthodes précises de protection pour l'étiquetage des données délicates, le verrouillage des classeurs, etc. Ces problèmes de la protection sont les mêmes que pour tout système manuel.

7. Pratiques courantes et estimation des coûts

Les systèmes de programmation actuels ne comportent guère, pour la plupart, que des dispositifs élémentaires de sécurité. C'est vrai qu'il y a peu d'exigences sous ce rapport. Les systèmes à cote de sécurité élevée fonctionnent dans des zones isolées et protégées où toutes les données sont considérées comme confidentielles. Dans ce cas, il n'y a pas de véritables besoins de vérification par programmerie bien au point.

Les réponses au questionnaire ont révélé beaucoup d'intérêt pour les mesures de sécurité. Le questionnaire ne s'adressait qu'à ceux qui disposaient d'ordinateurs. Parmi les 475 qui ont répondu à la question relative à la protection, 72 p. 100 exerçaient un certain contrôle sur l'accès physique, 38 p. 100 appliquaient des mesures de sécurité telles que les mots clés ou le codage, 42 p. 100 soumettaient à des vérifications l'intégrité de leur personnel, 57 p. 100 employaient les livres de vérification ou d'autres moyens de contrôle, et 68 p. 100 réglementaient la destruction des données.

Récemment, on a consacré plus d'effort aux mesures de protection dans le cadre du travail en temps partagé. Le personnel du Groupe d'étude a eu l'occasion d'étudier les modes de protection chez un façonnier. Ce type d'entreprise n'est pas typique, car il a plus de motifs pour vouloir assurer un cadre de protection au traitement des données; leur survie dépend en grande partie de leur aptitude à sauvegarder le caractère confidentiel des informations de leurs clients. Cet examen aura cependant été utile; il aura permis d'apprécier les méthodes de protection en usage dans le commerce. Voici celles qui ont été notées :

Sécurité physique. — Tous les employés portent des insignes très apparents. Les portes d'accès aux ordinateurs sont munies de serrures à combinaisons de dix boutons et en tout temps au moins quatre opérateurs sont en fonction. L'opérateur principal vérifie l'accès à la zone de calcul et veille à ce que le régistre des entrées soit tenu à jour. Le système enregistre automatiquement les interventions de l'opérateur, notamment le montage des bandes.

Méthodes de sécurité. — Il y a un responsable de la sécurité des données et un suppléant; tous deux relèvent du chef d'exploitation

des systèmes. Le responsable assigne les mots clés et dirige la programmation des pratiques spéciales de sécurité. Tout le personnel informatique a été soumis aux contrôles sécuritaires établis par le ministère fédéral des Approvisionnements et Services.

Fichiers. – On vérifie sur les cartes de travail les demandes d'accès aux rubans ou aux disques. Un programme d'index automatisé contrôle le numéro de série du ruban d'après les numéros de compte de l'utilisateur et imprime son résultat sur des pupitres de commande dans la bandothèque. Si les numéros de compte du propriétaire et du demandeur ne coïncident pas, on vérifie dans un fichier manuel si le demandeur a reçu une autorisation écrite du propriétaire à employer le fichier, ou bien si des instructions définies de l'utilisateur porteraient sur la protection. On tient un registre des explorations de la bandothèque.

Télétraitement. – Le pointage du début se fait suivant un mot clé. Les mots clés changent par intervention administrative. Il n'y a pas de vérification d'identité pour les terminaux des circuits à débit lent; l'utilisateur doit alors transmettre son numéro de compte, établir son identité et donner le mot clé. L'accès est restreint aux fichiers portant l'identification de l'utilisateur. On tient un registre de l'accès aux terminaux avec pointage d'arrivée et de départ.

Codage. – Les données provenant de terminaux à distance sont brouillées par transformation simple pour stockage temporaire. Elles sont déchiffrées pour les calculs puis rebrouillées pour stockage temporaire, enfin déchiffrées avant d'être livrées à l'utilisateur; ainsi les données qui sortent correspondent à la commande. On ne voit pas dans le captage des messages sur lignes de télécommunication de risques sérieux.

Ces techniques ne représentent pas le fin mot en matière de sécurité. D'après le façonnier interviewé, elles constituent un moyen terme entre la protection que le consommateur exige et le prix qu'il est prêt à payer.

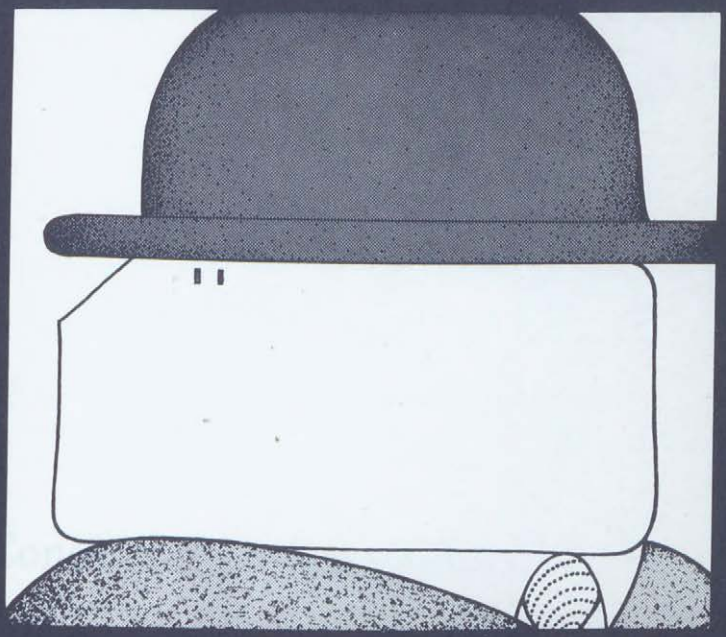
À plusieurs reprises on a estimé le coût d'une protection raisonnable des données pour traitement en temps partagé, ou traitement séquentiel à distance. Une étude menée par le Groupe a révélé que l'on pouvait offrir une bonne protection pour 3 p. 100 des frais de stockage et 12 p. 100 de la valeur du temps d'exécution de l'unité centrale. Ce système permettait notamment la séparation des en-têtes des données elles-mêmes, l'effacement des données utilisées, le codage des données et une épreuve pour s'assurer qu'elles n'ont pas été changées sans autorisation. Il ne fournissait pas de protection à l'échelon des zones comprises dans un enregistrement. Le chiffre de 12 p. 100 est conforme en général à

bon nombre d'autres estimations. Les prévisions les plus basses quant aux coûts supplémentaires des mesures de sécurité sont de l'ordre de 5 p. 100 ; les plus hautes se rapprochent de 15 p. 100. La société I.B.M. annonçait récemment son intention d'investir $ 40 millions au cours des prochaines années dans la mise au point d'équipements et de programmeries de protection pour ses ordinateurs.

En définitive, les mesures de protection relèvent de l'entreprise qui manipule les données. Cependant, il y a lieu de faire un parallèle avec l'industrie automobile, comme le déclarait à quelques membres du Groupe d'étude un représentant de l'organisme américain dit *Senator Ervins's Sub-committee on Constitutional Rights* ; ainsi il incomberait aux fabricants de matériels informatiques de fournir « ceintures et freins de sécurité », c'est-à-dire les moyens nécessaires à une protection raisonnable, et d'initier les clients à leur emploi.

[1] La substance de ce chapitre est empruntée à l'étude effectuée pour nous par C. C. Gotlieb et J. N. P. Hume et intitulée *Systems Capacity for Data Security.*

Quatrième partie



Les secteurs névralgiques

Chapitre 10
Le traitement de l'information et l'individu

1. Considérations générales

En traitant, dans les chapitres qui précèdent, de la diffusion et du stockage des renseignements de caractère intime, nous avons dégagé la relation complexe qui s'établit entre la vie privée et l'information. Une bonne partie des questions soulevées portent directement sur la vie privée et les valeurs qui s'y rattachent, alors que d'autres n'ont trait en réalité qu'au pouvoir découlant de la possession des données.

Même si avec l'*Ontario Medical Association* on estime que « ce sont les gens qui envahissent la vie privée et non pas les ordinateurs », il n'en reste pas moins que les ordinateurs influencent et même parfois déterminent les manières dont les gens peuvent envahir la vie privée. En raison même de leur efficacité, les ordinateurs font tomber une bonne partie de la protection qui, faute du même rendement, existait jusque-là. Par exemple, les ordinateurs facilitent la fusion des divers dossiers personnels de l'individu en un dossier global. On peut acheminer presque partout

et à un prix relativement bas, surtout si on a recours aux télécommunications, des quantités de données à peu près illimitées. D'où les craintes, excessives parfois, que l'ordinateur occasionne la manipulation des hommes, détruise toute possibilité de vie privée et réduise l'homme à un numéro. Dans l'enquête du ministère des Communications, 62 p. 100 des sujets ont souscrit à l'énoncé ci-après : « du fait des ordinateurs, les individus sont en train de devenir des numéros ». La pression qui s'exerce déjà en différents milieux administratifs et politiques canadiens en faveur d'un système d'identification à numéro unique contribue sans aucun doute à cette inquiétude.

L'enquête du Groupe d'étude a révélé que la plupart des fichiers à données strictement personnelles ne sont pas encore automatisés ; or, tous les grands systèmes d'information présentent déjà pour la vie privée et les valeurs connexes des dangers réels, et l'automatisation ne pourrait que les intensifier. Les renseignements contenus dans une chemise ou simplement griffonnés au dos d'une enveloppe peuvent faire autant de tort, utilisés à mauvais escient, que les plus imposantes feuilles de sortie d'ordinateur.

Puisque l'automatisation, en progrès rapide, a sensibilisé les gens à ces dangers, sans pour autant avoir rendu les problèmes insurmontables, il semble donc opportun d'examiner sous ce rapport l'ensemble des systèmes d'information. Bien que 53 p. 100 des enquêtés estiment que « les ordinateurs vont porter atteinte au caractère confidentiel des données » et bien que le débat suscite de plus en plus de participation et d'intérêt dans nombre de pays (surtout au niveau des gouvernements), le problème n'a pas encore atteint selon nous des proportions alarmantes. Le Groupe d'étude estime toutefois que la situation pourrait s'aggraver rapidement et reconnaît avec d'autres observateurs le danger que le grand public se désintéresse de cette question, comme pour d'autres problèmes sociaux.

L'ampleur des problèmes qui se posent semble sans rapport avec leur caractère public ou privé. L'élément décisif serait la nature de l'information elle-même. Les méthodes des corps de police et des agences d'enquêtes commerciales, par exemple, se ressemblent parce que les renseignements qu'ils manipulent sont de types similaires.

Les personnes en quête de travail, de logement, de crédit ou d'assistance sociale sont amenées à fournir nombre de renseignements personnels qui forment la grande partie des données recueillies et traitées actuellement. Il leur faut s'y résoudre pour obtenir les avantages qu'elles recherchent. À cet égard, le cas des

programmes d'aide sociale est particulièrement important puisqu'il entraîne la mécanisation de données concernant un nombre croissant de gens qui se trouvent, par la force des choses, dans une situation de dépendance marquée. L'efficacité de ces programmes est liée à celle des méthodes de collecte et de traitement de l'information ; mais ne faut-il pas craindre qu'une érosion croissante de la vie privée en soit le prix.

Le Groupe d'étude, faute de ressources, ne s'est pas mis en quête d'exemples qui eussent établi le bien-fondé des allégations d'immixtion dans la vie privée. Il en a suffisamment appris cependant pour savoir à peu près dans quelles occasions l'intimité des personnes risque d'être battue en brèche.

2. Collecte des données

Dans le mandat du Groupe d'étude, l'examen détaillé des pratiques et des méthodes de collecte de données n'était pas primordial. Néanmoins, la collecte des données intéresse la vie personnelle. Elle suppose qu'on obtienne les renseignements des personnes concernées ou de leurs voisins, de leurs employeurs, de leurs amis. Le Groupe d'étude a constaté lors de ses enquêtes que la plupart des banques d'information sont dénuées de directives précises touchant le genre d'information à recueillir pour se conformer aux objectifs assignés. Il y a peu de garanties contre la tendance des grandes entreprises et surtout des organismes publics à rassembler plus de données que n'exigent les fins immédiates ou contre la collecte de renseignements qui puissent servir plus tard de fondement à la discrimination raciale, religieuse ou autre. Il n'existe non plus ni limites ni règles concernant les sources des données ; l'opinion publique a cependant réagi devant les procédés de certains enquêteurs qui font des investigations non autorisées chez les amis et les voisins d'un individu, ce qui fait que le dossier final dépend, en partie, de ouï-dire et de potins pas nécessairement exempts de préjugés et de malveillance.

Le Groupe d'étude a également constaté que la collecte des renseignements est souvent confiée aux employés les moins formés et les moins rétribués. En outre, ceux qui collectent les données, à l'exception évidemment de certains organismes tels que Statistique Canada, sont souvent envoyés sur le terrain ou dans les foyers avec de très vagues recommandations quant à la manière de se conduire, surtout en ce qui concerne le caractère confidentiel des données.

3. Le contenu des fichiers personnels

Il est au moins quatre cas où les renseignements consignés dans des fichiers peuvent occasionner des difficultés : quand ils sont déshonorants, nuisibles, inexacts ou non pertinents. Le Groupe d'étude a également noté le peu de directives d'ensemble ayant trait à ces questions et, en général, au contenu des fichiers.

Peu d'organisations s'adonnent à la collecte de données déshonorantes commme une fin en soi, en dehors des agences d'enquête et de renseignements. Pourtant, des informations de cette nature sont effectivement collectées et classées. Jusqu'ici rien ne semble y faire obstacle. La loi contre la diffamation, malgré l'étendue de son champ d'application, n'empêche pas en général que l'information diffamatoire soit recueillie et même diffusée, pourvu qu'elle soit vraie.

L'information nuisible diffère de l'information déshonorante en ce qu'elle ne cause de torts qu'en certaines circonstances. Ainsi, le fait de divulguer l'âge d'une personne, qui n'est pas un facteur d'abaissement, pourrait l'empêcher d'obtenir certains emplois. L'information nuisible, qui à proprement parler, ne concerne pas la vie privée, s'y rattache étroitement comme l'information diffamante. En effet, elles se confondent souvent ; ainsi, lorsqu'on fait part à un directeur de banque des tendances alcooliques de l'un de ses clients.

Que l'information inexacte soit nuisible ou non, elle peut causer des ennuis. Il a été établi que les banques d'information renferment plus de renseignements inexacts qu'on ne le croit généralement. L'échange de plus en plus fréquent de données entre banques d'information peut causer préjudice en plus d'une occasion, et cela à cause d'un seul élément inexact. On mettra sans doute au point des techniques et des mesures profitables à un éventail de valeurs et d'intérêts, y compris le respect de la vie privée, en corrigeant les inexactitudes.

Finalement, il faudra formuler des directives touchant la pertinence de l'information dans les fichiers et l'information désuète ou inutilement détaillée. Celles-ci auraient trait aux types de données qui se rattachent à des fins déterminées ainsi qu'à l'élimination des fiches périmées, tels le casier judiciaire ou le défaut de paiement, de sorte que le passé d'un individu ne le poursuive pas à jamais.

4. Stockage et manipulation des données

Le Groupe d'étude a constaté que de nombreuses banques d'information ont programmé des normes et des règles de sécurité pour se protéger contre les fuites et restreindre au personnel autorisé l'accès à certains fichiers. D'autres cependant ne se sont pas beaucoup intéressées à cette question. En fait, bon nombre de celles qui ont adopté des mesures de sécurité n'avaient pas pour motif principal le respect de la vie privée. De toute façon, on semble devenir plus conscient de la nécessité de protéger les données.

L'efficacité des normes techniques de sécurité met en lumière un point souvent négligé jusqu'ici : l'efficacité de l'ordinateur, inquiétante sous un certain angle, peut justement servir des fins opposées, dont la protection de la vie privée. Il est plus facile d'appliquer des normes strictes de sécurité à des systèmes d'information automatisés qu'à des systèmes manuels. De plus, il est possible de maintenir un livre de vérification qui tienne compte de chaque emploi d'un fichier; il est alors très simple de fournir des feuilles de sortie si l'intéressé lui-même veut les examiner. Enfin, le fait même que les ordinateurs constituent une cible aussi visible, tant au plan matériel que politique, peut faciliter la tâche de ceux qui cherchent des moyens d'assurer le respect de la vie privée.

On ne peut parler de sécurité sans soulever la question de la négligence. On peut tout aussi bien porter atteinte à la vie privée par manquement qu'à dessein : on laissera à la vue des fichiers confidentiels; l'enquêteur parlera sans raison de gens qu'il a interviewés; le recenseur se livrera à des indiscrétions au sujet de renseignements obtenus chez quelqu'un du voisinage. La formation et la surveillance du personnel des banques d'information permettraient de réduire au minimum ce genre de « fuites ».

5. Diffusion des données

Les critères s'appliquant aux personnes ou aux organisations vers lesquelles une information peut être acheminée, les conditions qui réglementent cette diffusion ou cet échange et les méthodes de distribution varient d'une banque d'information à l'autre. Certaines banques d'information, dont Statistique Canada, se voient interdire par la loi la diffusion ou la publication de toute information relative à des individus identifiables. Dans le secteur privé, et

aussi dans le secteur public (bureau provincial de permis de véhicules automobiles, par exemple), certains dirigeants de banques d'information, estimant détenir un certain droit de propriété, se croient fondés à mettre le contenu des fichiers à la disposition de tiers. Ils considèrent généralement que c'est une affaire qui les regarde seuls. C'est ainsi qu'une personne ayant fourni librement des informations destinées à des fins précises (demande de permis, de bail, etc...) pourra apprendre que ces informations circulent en d'autres milieux et sont utilisées à des fins tout autres. Ainsi, un nom et une adresse donnés dans tel dessein seraient utilisés à des fins de sollicitation commerciale. Un dossier médical, s'il expose un cas rare, peut aboutir à la salle de conférences. Les organismes publics ont une responsabilité toute spéciale quant aux précautions touchant la diffusion des renseignements, puisque souvent ils seront habilités à en faire la collecte. En général, les gouvernements sont de loin les plus grands collecteurs de données, agissant au nom de « l'intérêt public ». Aussi, doivent-ils, dans l'intérêt public, assurer le caractère confidentiel de ces données.

Pour la collecte des données, la plupart des banques d'information s'adressent à l'intéressé ; ce dernier fournit lui-même l'information ou en autorise la collecte. Dans ces cas-là, et jusqu'à ce que cette information soit transmise à un tiers, en particulier à une autre banque d'information, l'individu connaît vraisemblablement les raisons pour lesquelles on a recueilli les renseignements le concernant et l'utilisation qui en est faite. Cependant, une fois que l'information passe à un tiers, l'individu, même s'il est au courant ou a donné son autorisation (mais davantage s'il ne la donne pas), perd toute trace de cette information et le sentiment d'en avoir eu la maîtrise.

Toute la question de la diffusion des données personnelles exige une attention spéciale et des mesures précises comme celles que prévoit le *Personal Investigations Act* du Manitoba.

6. L'accès aux données

Quant à savoir si les individus devraient avoir accès à leur propre fiche, on note une très grande diversité d'opinions. Selon l'enquête du Groupe d'étude, la majorité des dirigeants de banques d'information estiment que les intéressés ont le droit de savoir qu'il existe une fiche à leur sujet et d'en connaître le contenu. Cependant, ce « droit » n'a pas été très bien respecté jusqu'ici. Ce n'est que depuis peu, par exemple, que les agences de renseignements commerciaux ont pour règle de permettre aux particuliers de voir

leur dossier ; au Québec, en Saskatchewan et au Manitoba la loi les y oblige.

Mais il n'y a plus accord quant à établir si l'individu doit être autorisé à porter à un dossier les objections qu'il estime appropriées (droit que les lois des provinces susmentionnées reconnaissent) et à exiger corrections, précisions, suppressions ou ajouts.

Les avis diffèrent également sur la question de savoir si la personne doit être prévenue chaque fois que l'information passe à un tiers, s'il faut identifier ce tiers et, de plus, si elle doit avoir le droit de contrôler la diffusion ultérieure de l'information la concernant. Autre point de divergence, faut-il accorder à l'individu le droit de connaître les sources de l'information qui le concerne ?

De l'avis du Groupe d'étude, les conditions d'accès peuvent susciter des difficultés. Les frais peuvent être fixés à un niveau prohibitif ; l'avantage sera bien mince pour l'individu si la feuille de sortie de son dossier comporte des informations en symboles alphanumériques ; les demandes d'accès peuvent devenir abusives. Suivant certaines propositions, les banques d'information enverraient régulièrement une feuille de sortie à chaque intéressé. Il est fort possible d'ailleurs qu'un petit nombre seulement souhaitent vérifier leurs dossiers.

Les points importants et controversés que soulève la question de l'accès aux données doivent être examinés avec la plus grande attention. Il importe de poser en principe le droit d'accès pour le particulier aux fiches qui le concernent et de faire en sorte que l'exercice de ce droit soit possible en tout ce qui a trait au respect de la vie privée. Les solutions seront aussi diverses qu'il y a de genres de fichiers.

7. L'État et la vie privée

À maintes reprises, dans les pages qui précèdent, nous avons indiqué que certaines valeurs, certains intérêts moraux, certaines exigences – notamment le respect de ce qui est confidentiel – sont immédiatement reliés à la vie privée, tandis que d'autres, dont l'exactitude de l'information, s'en distinguent conceptuellement même s'ils s'y rattachent sur les plans subjectif et pratique.

Par delà l'expression « respect de la vie privée » qui embrasse toute la gamme des préoccupations de cet ordre, qu'elles aient ou non des liens directs avec la notion de vie privée, certains emploient librement cette formule dans le débat sur l'ordinateur et la vie privée pour évoquer un type de préoccupation d'une portée plus vaste et plus fondamentale qui trouverait son origine dans les

frustrations nombreuses – injustices sociales, aspirations politiques déçues – inhérentes à une société complexe, institutionnalisée et impersonnelle.

La formule « privacy is power » (manifestement calquée sur l'expression « information is power »), utilisée par Weisstub et Gotlieb dans leur étude pour le Groupe, indique la nature de ces préoccupations. Évidemment l'observation repose sur un jeu de mots. Dans la société post-industrielle, l'information tient une place prépondérante. Elle sera peut-être la clé des décisions. Ceux qui la détiennent seront avantagés à cet égard ; les autres seront gênés sous ce rapport, voire impuissants à prendre part aux décisions d'autrui les concernant. « Respect de la vie privée » en vient ainsi à évoquer des préoccupations globales, souvent confuses et mal formulées, qui vont du souci de la somme des renseignements que l'on collecte sur des individus à la crainte que la possession de ces données accroisse largement les pouvoirs de manipulation et de propagation du conformisme que détiennent les maîtres de l'information.

Le débat actuel sur la pollution du milieu offre une analogie. L'étendue de la protestation indique peut-être que le public ne se soucie pas simplement de l'environnement physique mais aussi de l'environnement social et politique où la recherche du profit se fait au détriment de la qualité de la vie.

L'analogie est parfois odieuse, surtout si elle est établie avec un sujet qui soulève autant de passion. Néanmoins, le parallèle peut être utile dans la mesure où il montre que le débat sur le respect de la vie privée est peut-être mal engagé. Peut-être les atteintes à la vie privée, au sens classique du terme, inquiètent-elles moins que les menaces planant sur la liberté individuelle et l'autonomie de la personne du fait de systèmes d'information éminemment efficaces.

Les ordinateurs ayant tant monopolisé l'attention, il convient de rappeler que le développement prodigieux que connaît la collecte de l'information a précédé leur invention et leur application. Les gouvernements rassemblaient des données pour lever les impôts, réprimer les rébellions et, plus tard, gérer les programmes d'assistance sociale et de péréquation des revenus. Le secteur privé, s'étant avisé de la valeur commerciale de l'information exacte et immédiatement accessible, s'engagea dans la même voie. Plus récemment, les spécialistes des sciences sociales et des études de marchés ont déterminé une troisième vague de collecte et d'analyse des données.

Ainsi se créait une industrie qui atteint maintenant une taille gigantesque. Une autre tendance, quelque peu opposée, se fait jour,

comme le font observer Weisstub et Gotlieb : « Les aspirations de l'homme moderne à la connaissance ont atteint des proportions démesurées ». Bref, le niveau des exigences individuelles s'est haussé considérablement. Aussi, pour répondre aux attentes exprimées, les organisations ont mis sur pied des programmes destinés à servir les citoyens. À cette fin, elles doivent recueillir des masses de renseignements sur les particuliers et les choses, et en tirer subséquemment avantage pour elles-mêmes.

Il n'y a pas lieu d'examiner dans le présent rapport le comportement des organisations, si bienfaisantes qu'elles aient été à l'origine, ni à nous demander si elles ne tendent pas après un certain temps à créer de nouveaux besoins pour justifier leur existence et leur développement. Nous constatons cependant que de plus en plus de gens posent la question et avec plus d'insistance que jamais. En l'occurrence, l'information joue un rôle majeur. Les systèmes d'information semblent accroître l'efficacité, et par conséquent la puissance des organismes qui les exploitent. Ceux qui contestent l'autorité de ceux-ci, ou du moins la manière de l'exercer, invoquent généralement le respect de la vie privée, mais en fait s'attaquent au pouvoir des organisations et à ses liens avec l'information.

Le débat embrasse aussi le rôle de l'ordinateur, mais il est moins chargé alors, quoique révélateur. Qu'il ait pour thème « l'ordinateur et la vie privée » et non la *vie privée* seulement, est en soi significatif. L'ordinateur excelle dans le traitement de l'information quantifiable et systématisable ; celle qui est intuitive, ambiguë, irrationnelle ne se laisse pas mécaniser aisément. En conséquence, il renforce la position du technocrate aux dépens de l'humaniste dans le processus décisionnel, assurant la préséance de l'objectif sur le subjectif. Pour illustrer l'un des effets politiques virtuels de l'ordinateur, A. Downs [1] signale une conséquence de son emploi grandissant :

> « L'administration dans son ensemble y gagne aux dépens du corps électoral... Les groupes organisés et efficaces acquièrent de la puissance aux dépens de ceux qui le sont moins... Les fonctionnaires de formation technique accroissent leur autorité aux dépens des conseillers politiques de l'ancienne école. »

En effet, les individus non organisés, non technocrates, c'est-à-dire le commun des mortels, sont comme dépouillés de leurs droits par ce phénomène.

C'est, en résumé, le pressentiment d'un cauchemar technocratique, alimenté par la simplification à outrance et la spéculation

pure. D'ailleurs ce dont les ordinateurs sont capables et ce qu'ils font véritablement sont deux choses tout à fait différentes. Sauf peut-être dans quelques sociétés multinationales, les ordinateurs, en particulier les fameux systèmes de gestion automatisée, ont eu peu d'effets sur le comportement des organisations. D'après les constatations du Groupe d'étude sur la téléinformatique, ces systèmes n'ont pas répondu aux attentes, en règle générale. Fait aussi important, les ordinateurs peuvent rendre les informations accessibles à tous, si telle est la volonté de l'État.

Toutes ces considérations touchant le respect de la vie privée ont chargé l'expression d'inquiétudes sociales, se rattachant toutes au fait de détenir l'information ou d'en être privé. Ces préoccupations semblent prendre racine dans le pressentiment que l'individu sera impuissant face aux organisations omniscientes, qu'il sera manipulé ou réduit à un matricule, et obligé de se soumettre.

Selon une des propositions les plus fréquentes chez ceux que touche l'aspect politique dans les débats sur la vie privée, il faut que les individus aient droit d'accès non seulement à l'information les concernant, mais au nom d'un meilleur équilibre du pouvoir dans la société, à l'information portant sur les organisations auxquelles ils se heurtent. Certains militants iraient même plus loin, soutenant que la meilleure façon d'atteindre leurs objectifs serait d'abolir tout caractère privé, qu'il s'agisse d'organismes ou de particuliers, de sorte que l'information et la puissance politique qu'elle confère soient réparties également. Dans un rapport au Groupe d'étude, Claude Fabien notait :

> « L'objectif du contrôle des agents agresseurs de la vie privée, c'est ultimement d'atténuer ces frustrations, de diminuer les tensions qui en résultent entre l'État et le citoyen, entre l'organisation économique et le consommateur, entre l'employeur et l'employé. L'objectif, c'est en réalité la paix sociale. »

8. La liberté d'information

Nous avons traité dans la section précédente du droit pour l'individu d'accéder à l'information que détiennent les organisations afin d'assurer un meilleur équilibre social entre l'un et l'autre. Le public réclame de plus en plus d'informations aux gouvernements et aux entreprises, estimant que ces derniers doivent lui rendre compte de leurs décisions et voulant participer davantage aux affaires publiques.

L'individu, pour sa part, réclame en tant que citoyen la

« liberté d'information » ou le « droit d'être informé », tout en exigeant à titre personnel le « respect de la vie privée ». Il faut donc chercher des accommodements. La sauvegarde de la vie privée interdira en certaines occasions la divulgation de certains renseignements. Par contre, il faudra parfois sacrifier le respect de la vie privée aux intérêts supérieurs de la société.

Le conflit ne sera pas toujours aussi tranché entre ces deux droits. Diverses situations exigent des solutions nuancées où chacun trouve sa juste part. Il peut arriver que, pour une bonne planification sociale et plus d'efficacité, ou tel besoin social, les gouvernements et les entreprises doivent recueillir des données touchant diverses questions que l'individu estimera de caractère privé ou immédiatement reliées à ses intérêts financiers. Il ne s'ensuit pas nécessairement que l'État ou l'entreprise soient autorisés à rendre cette information publique, en vertu d'une certaine conception abstraite de « la liberté d'information ». Là encore, un citoyen peut avoir une excellente raison pour prendre connaissance d'un dossier ou d'un document gouvernemental, renfermant des données qui l'intéressent personnellement, mais son intérêt même légitime devra être mis en balance avec ceux d'autres personnes si le document renferme aussi des données personnelles sur leur compte ou révèle leurs opinions.

Manifestement, aucune formule générale et abstraite ne peut trancher le conflit entre la « liberté d'information » et le « droit à la vie privée ». Au contraire, il s'agira de réaliser de délicates pondérations selon les circonstances. Sans doute, serait-il possible de formuler des principes directeurs à cet égard, mais cela dépasserait les limites de notre mandat. Une politique de « la liberté d'information » pourrait faciliter les choix en cette matière.

9. Résumé

Les questions politiques n'entrent pas dans le cadre du mandat du Groupe d'étude. Cependant, une appréciation du malaise que créent l'efficacité et la pénétration des systèmes d'information, qu'ils soient ou non coupables d'immixtion dans la vie privée, permet d'expliquer la persistance de l'intérêt public pour la question.

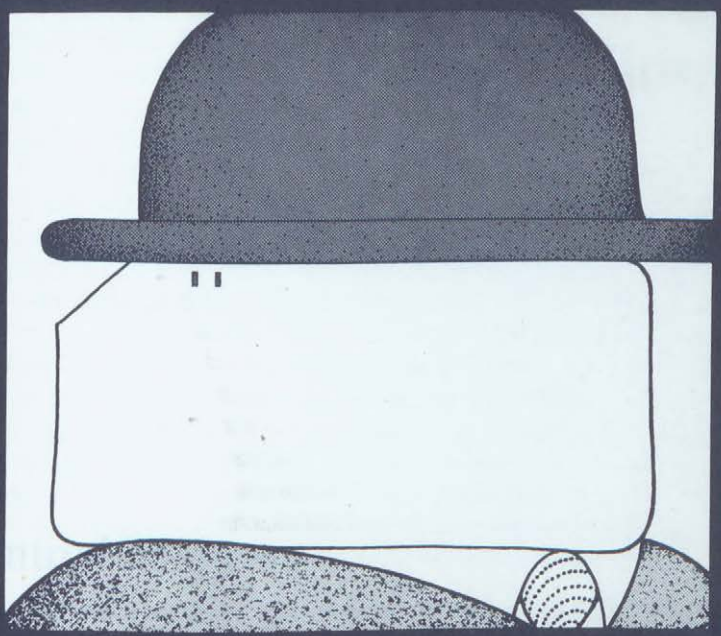
La mission du Groupe d'étude se rapporte plus immédiatement à des préoccupations bien définies : exactitude, pertinence, contrôle de la diffusion des données, normes de sécurité, accès et directives générales touchant les méthodes de collecte. De l'avis du

Groupe d'étude ces points doivent faire l'objet d'une réglementation visant les banques d'information qui renferment des renseignements strictement personnels sur des individus identifiables.

Le Groupe d'étude estime important de souligner, sur la foi des réponses au questionnaire touchant le respect de la vie privée, que la plupart des dirigeants de banques d'information sont prêts à accepter des mesures raisonnables de protection. Peut-être ce fait traduit-il de l'inquiétude face à un péril auquel ils seraient eux aussi exposés éventuellement ; c'est qu'ils figurent, en tant qu'individus, dans une banque d'information dépendant de quelqu'un d'autre. Par contre, les normes de protection qu'ils acceptent volontiers ne sont peut-être que le prix à payer en toute prudence pour désamorcer la controverse. De toute façon, l'intérêt qu'ils ont manifesté a dépassé notre attente.

[1] DOWNS, A, « The Political Payoffs in Urban Information Systems », dans *Information Technology in a Democracy*, publié sous la direction de Westin, Harvard, 1971, pp. 311-321.

Cinquième partie



La vie privée et la législation

Chapitre II
Droit et caractère privé de l'information

1. Introduction

Quand on aborde la question de la vie privée en droit canadien, on constate qu'elle a fait l'objet de bien peu de recours. Ce fait étonnera peut-être les partisans de solutions juridiques dans le débat sur l'ordinateur et la vie privée, d'autant plus que les États-Unis, pays avec lequel nous avons un grand nombre de valeurs en commun, offrent un contraste marqué avec le Canada sous ce rapport.

On sait que les États-Unis ont un système de *Common law* semblable à celui de toutes les provinces canadiennes, sauf le Québec qui est régi par le Code civil; les tribunaux y ont élaboré un ensemble imposant de lois sur la vie privée depuis 1890[1], année où la *Harvard Law Review* publiait un article de Warren et Brandeis concernant le droit à la vie privée. Ne soyons pas trop surpris toutefois de cette situation. Roscoe Pound n'a-t-il pas noté que des intérêts sociaux, tel celui de la vie privée, « ne sont pas créés, mais simplement reconnus par la loi[2] ». Pour que le droit

tienne compte d'une revendication sociale, il faut que la société en ait reconnu jusqu'à un certain point la validité.

Nous avons vu que le souci de la vie privée ne se fait pressant que depuis quelques années, phénomène largement attribuable à l'urbanisation et au caractère post-industriel de notre société. Auparavant une bonne partie de l'existence se déroulait au sein de la famille et parmi les voisins à l'abri de l'observation scrutatrice. On ne considérait guère comme violations de la vie privée que les immixtions dans la jouissance de la propriété et de l'intimité du foyer, et les atteintes à la réputation. Dans les circonstances, les lois contre l'intrusion (trespass), le trouble de jouissance (nuisance) et la diffamation assuraient la protection du milieu matériel de la vie domestique et sociale.

Les questions de vie privée relevant directement du Groupe d'étude se rattachent cependant à la crainte que des renseignements personnels puissent être diffusés dans le commerce ou l'administration publique à l'insu de la personne intéressée et lui causer éventuellement des préjudices.

On sait que les États-Unis se sont urbanisés et hautement industrialisés bien avant le Canada ; cela expliquerait en partie le rôle de précurseur qu'ils ont joué dans l'élaboration du concept juridique de *vie privée*. Mais l'explication ne suffit pas, car notre *Common law* est fondée pour une bonne part sur celle de Grande-Bretagne, pays hautement urbanisé depuis longtemps. Il faut donc chercher d'autres raisons au retard du Canada. Cela tient peut-être simplement à des situations sociales différentes dans les deux pays. En effet, les mœurs jouent un rôle important dans l'élaboration du droit. L'une des différences, et non la moindre, réside dans l'attitude à l'égard du droit et des tribunaux comme moyens de résoudre des conflits d'ordre social. Aux États-Unis, on recourt davantage aux voies judiciaires et les cours innovent plus, les deux phénomènes étant probablement causes et effets. Cette évolution a sans doute été intensifiée par l'influence de la constitution, où sont exprimées nombre de valeurs fondamentales du pays, dont quelques formes de droit à la vie privée. La constitution canadienne, par contre, ne fait guère que délimiter les domaines de compétences politiques.

Le concept de *vie privée* évoque trois sphères où l'individu peut prétendre à la faculté d'agir comme il l'entend, ainsi que nous en faisions état au chapitre premier. Ces sphères consistent en des lieux délimitables que l'individu peut vouloir quitter ou occuper sans dérangement ; dans l'espace de sa personne physique que le droit protège d'un caractère d'inviolabilité ; dans la sphère morale

où il peut vouloir se protéger contre toute communication de renseignements à autrui, notamment par l'écoute clandestine. Ces trois exigences, bien sûr, peuvent se heurter à des revendications contraires.

C'est à la troisième notion de la vie privée – relativement à la collecte, au stockage et à la diffusion de l'information personnelle – que le Groupe d'étude s'est intéressé au premier chef.

Deux stades de l'information, définis plus haut dans le Rapport, correspondent *grosso modo* à ce que désignent les termes « entrée » et « sortie » en jargon informatique. Le premier est celui de la collecte des données ; la vie privée est alors en jeu, car des faits concernant un individu sont portés à la connaissance d'une autre personne. Cette étape soulève la question de la méthode de collecte et de la nature des données. Le deuxième stade, plus important du point de vue du Groupe d'étude, consiste dans la diffusion des données ; alors des renseignements personnels peuvent être communiqués à des tiers ou au public, soit délibérément, soit par inadvertance, faute de mesures de sécurité suffisantes.

La *Common law* et le droit civil répondent aux nouvelles exigences sociales de par leurs principes fondamentaux. La *Common law* adapte aux situations nouvelles les recours qu'elle comporte ou en crée de nouveaux. Les civilistes cherchent à déterminer comment les principes du Code, notamment en matière de délit, s'appliquent aux circonstances nouvelles. Les deux régimes juridiques tentent de s'adapter à une époque de création et de mutation dans le domaine des valeurs.

Le droit canadien ne reconnaît pas de droit général à la vie privée. Cependant, il a donné lieu, comme nous le verrons, à des innovations intéressantes, notamment en Colombie-Britannique, au Manitoba, en Saskatchewan et au Québec. D'ailleurs, certaines sphères du droit protègent indirectement la vie privée. Si le concept de la vie privée n'est pas généralement reconnu par le droit canadien, il ne s'ensuit pas qu'il y ait absence de garanties juridiques à cet égard.

D'une manière très générale, les droits civils, qu'ils intéressent la personne ou la propriété, impliquent la reconnaissance de la vie privée, puisqu'ils comportent pour l'individu le pouvoir d'exercer des choix personnels, qu'il s'agisse notamment d'interdire l'accès de sa propriété ou de conclure des ententes contractuelles. Selon une interprétation plus étroite, certains domaines se rattachant à la vie privée font l'objet de droits et de recours définis. Les intérêts en cause peuvent être défendus par des actions civiles pour diffamation ou violation de foi ; ils sont en outre garantis par des lois

pénales interdisant les atteintes à la réputation et à la dignité de la personne, par les lois touchant la preuve pour ce qui est du caractère confidentiel de renseignements personnels découlant de certaines relations, et par diverses lois frappant de sanctions la divulgation de renseignements sauf dispositions juridiques à cet effet.

2. Collecte des données

Aux prises avec un préposé à la collecte des données, on peut évidemment s'abstenir de fournir des renseignements sur soi. En certaines circonstances, lorsque par exemple on sollicite un passeport, de l'assurance ou du crédit, on n'est pas obligé en loi de donner des renseignements, mais alors on doit renoncer à l'avantage recherché. Parfois aussi la loi impose la divulgation, notamment dans les cas de mandats de perquisition ou des obligations créées par les lois fédérale et provinciales de l'impôt sur le revenu et par la Loi sur la statistique.

D'autres lois, cependant, protègent l'individu contre certaines extorsions illicites de renseignements. Le Manitoba et la Saskatchewan ont promulgué d'importantes législations générales. Nous y reviendrons dans la partie consacrée à la diffusion des données, sujet se rattachant plus nettement à notre mandat. De plus, l'Ontario a adopté en 1965 une loi imposant la licence, à des conditions strictes, aux investigateurs privés[3]. En sont exempts toutefois :

> « les personnes qui recherchent ou fournissent des renseignements 1) sur les fiches de solvabilité des particuliers; 2) pour le compte d'employeurs quant aux titres et aptitudes de leurs employés ou employés virtuels; 3) quant aux titres et à l'aptitude d'un candidat à l'assurance ou à une caution, mais qui n'exercent pas par ailleurs la fonction d'investigateurs privés »

Une législation particulière interdit les intrusions dans les communications et la surveillance des individus, sauf autorisation en droit. La Loi sur la radio[4] (article 9, 2) interdit toute interception non autorisée de radiocommunications. Cependant, l'infraction consiste dans la diffusion ou la divulgation du message intercepté. L'article a notamment pour objet d'appliquer au Canada la Convention internationale des télécommunications en ce qui concerne le secret. La loi de la Bell Canada[5] interdit l'interception de communications téléphoniques. L'Alberta, le Manitoba,

l'Ontario, le Québec et la Nouvelle-Écosse ont adopté des dispositions analogues. La législation canadienne interdit, sous réserve des exceptions prévues par la Loi sur les pénitenciers, l'interception de lettres et leur ouverture, serait-ce par la police ou des organismes gouvernementaux.

Le projet de loi sur la protection de la vie privée[6], présenté récemment à la Chambre des communes, porte interdiction de l'interception non autorisée d'une « communication privée » par des moyens électromagnétiques, dont les tables d'écoute ou les branchements clandestins ainsi que par des dispositifs acoustiques, ou autres. La communication privée, soit orale, soit par télécommunication, s'effectue dans des conditions où celui dont elle émane peut raisonnablement compter qu'elle ne sera pas interceptée par des tiers.

À la question des tables d'écoute se rattachent celles du voyeurisme et de l'écoute clandestine. Le Code criminel[7] interdit de rôder sur une propriété ou de s'y introduire la nuit, de l'épier ou de la cerner, mais ces infractions ne comprennent pas le fait d'épier un voisin de chez soi au moyen d'une longue-vue, ni l'espionnage des locataires par le propriétaire. Ces intrusions ne sont pas expressément interdites, sauf peut-être en Colombie-Britannique et au Manitoba, où l'on a fait de la violation de la vie privée un délit (a tort) donnant lieu à des poursuites[8]. Toutefois, il arrive que la protection découle de la *Common law*, par exemple, lorsque cet acte comporte violation de propriété, préjudices ou négligence

3. Diffusion

La diffusion de renseignements à des tiers intéressait le Groupe d'étude au premier chef. La législation en la matière prévoit des recours, notamment en Colombie-Britannique, au Manitoba et en Saskatchewan. Toutefois, ce sont le Code civil et la *Common law* qui assurent l'essentiel de la protection. Dans les lignes qui suivent, nous tenterons de dégager les recours de droit civil et de *Common law*

a. Le Code civil québécois

Dans le régime québécois, il n'est pas nécessaire de prévoir tous les délits particuliers pouvant correspondre aux situations de fait pour donner lieu à une réparation en droit, mais il faut déterminer si les principes généraux du délit, fondés sur la notion de faute, s'appliquent à telle situation.

Une action sera intentée contre telle personne si sa conduite a constitué une faute selon les termes du Code civil, notamment de l'article 1053, ainsi conçu :

> Toute personne capable de discerner le bien du mal est responsable du dommage causé par sa faute à autrui, soit par son fait, soit par imprudence, négligence ou inhabileté.

Cet article permet une grande souplesse pour établir si une nouvelle activité (résultant par exemple du progrès technologique) est illégale et pour créer des droits et des obligations s'y rapportant. En matière de vie privée le droit du Québec a donné lieu dès 1957 à un arrêt significatif. Un annonceur avait lu, en ondes, une lettre déplorant la programmation et suggéré aux téléspectateurs de « remonter » celui dont elle émanait, le docteur Robbins, projetant son nom et son adresse à l'écran (affaire *Robbins c. la Société Radio-Canada*[9]). Par la suite, Robbins avait reçu livraison de commandes de provisions dont il n'avait pas besoin et s'était fait harceler de diverses façons. Le tribunal, jugeant cette conduite préjudiciable, en a tenu Radio-Canada responsable. La diffusion de la lettre portait atteinte à la vie privée de l'auteur en l'identifiant et en faisant connaître ses vues. Certains juristes ont soutenu que cette cause avait créé le droit de la vie privée au Québec.

Des applications plus traditionnelles de l'article 1053 peuvent aussi assurer la protection de la vie privée. La diffamation et la violation de foi y donnent donc lieu à des recours analogues à ceux de la *Common law.*

b. La *Common law*

La *Common law* pourrait bien, avec le temps, créer le concept général de délit en matière de vie privée. Pour le moment, toutefois, c'est sous les rubriques de la diffamation et de la violation de foi qu'elle offre la protection la plus immédiate, en ce qui concerne l'information. Toutes deux ont trait à des situations où des renseignements sur une personne sont communiqués bien qu'elle s'y oppose.

La diffamation ayant été érigée en délit, le citoyen est protégé contre les communications de nature à porter atteinte à sa réputation. Le droit en la matière se rattache donc à la notion de la vie privée car il embrasse la diffusion de renseignements sur une personne ; il sera souvent invoqué dans les affaires de cet ordre. Toutefois, ne visant que les *faux* renseignements, il ne touche pas

l'essentiel de la vie privée : il ne protège pas contre la communication de faits véridiques, même si des préjudices pour la personne en résultaient. La publication de faits exacts, bien que non assimilée à la diffamation en droit, peut constituer une atteinte à la vie privée.

La *Common law*, voulant que la réputation de l'individu ait des incidences sur ses relations avec autrui, tend à le dédommager du préjudice porté à celles-ci par une atteinte à sa réputation. Elle protège la dignité de la personne dans la mesure où elle tient à l'opinion d'autrui. Ce n'est pas l'outrage du mensonge (calomnie orale ou libelle) qui constitue l'essence du délit, mais le préjudice qui en découle. Toutefois, des indemnisations exemplaires ont souvent été imposées pour le simple fait d'outrage ou d'atteinte à la dignité, une fois la diffamation démontrée.

L'activité des agences de renseignements commerciaux montre les limites du recours en diffamation pour défendre la vie privée contre les abus de l'information. Ces agences offrent des renseignements auxquels on aura recours pour décider si telles personnes sont sûres ou non en matière de crédit. Elles travaillent sur des données censément établies, sur des faits liés à la situation financière de l'individu, dont le revenu et les dettes, ou à des traits de caractère qui pourraient influer sur la solvabilité et l'honnêteté.

Si on s'élève parfois contre l'information sur le crédit, craignant qu'elle ne porte pas atteinte à la vie privée, c'est que les renseignements peuvent être incomplets, non pertinents, inexacts, voire préjudiciables et que l'intéressé peut ignorer qu'un rapport est établi sur son compte, et par qui et comment. Pour que la loi contre la diffamation puisse s'appliquer, dans les circonstances les plus favorables, il faut qu'il y ait renseignements inexacts, que l'inexactitude équivaille à la fausseté et qu'il soit établi que les renseignements ont été communiqués à des tiers, conditions qui ne vont pas sans difficultés. Si le rapport ne renferme rien d'inexact, la loi sur la diffamation ne comporte aucun recours, quel que soit le préjudice. Elle ne prévoit rien pour ainsi dire qui empêche l'agence de diffuser des renseignements véridiques, peu importe ce qu'ils comprennent ou excluent, à qui et quand elle les communique et que la personne faisant l'objet de l'information soit ou non au courant. (Un autre recours possible dans les circonstances se rattacherait à la déclaration inexacte par négligence qui déjà constitue un délit, et dont il sera question plus loin.)

Néanmoins, l'existence en droit du délit de diffamation peut freiner la diffusion d'informations préjudiciables, et protéger ainsi la vie privée, car il y aurait risque de poursuites si les renseignements tenus pour vrais se révélaient faux. En outre, certaines causes

ont tendu à élargir la protection accordée en exigeant que les informations nocives soient rigoureusement exactes et non seulement en substance. Cette exigence découragerait les énoncés diffamatoires. Dans l'affaire de *Green c. Minnes*[10], un agent de recouvrement avait, au moyen d'une affiche jaune posée dans diverses parties de la ville, fait savoir que les demandeurs devaient de l'argent. Le fait était exact en substance, ainsi qu'en avait conclu le tribunal de première instance. Toutefois, la Cour d'appel statua à l'unanimité qu'il y avait eu diffamation parce que le montant indiqué sur l'affiche n'était pas d'une exactitude absolue. Elle aurait été influencée, semble-t-il, par sa désapprobation de la méthode de recouvrement dont la publication de renseignements de nature à nuire.

Enfin, les tribunaux ont statué que, dans les cas d'information erronée, l'agence de renseignements commerciaux ne peut invoquer pour se défendre le « qualified privilege » en se déclarant tenue de communiquer l'information à ses clients. C'est là un domaine où le droit canadien protège mieux la personne que celui des États-Unis, où le privilège susmentionné peut intervenir dans la défense. Mais les services de crédit de deux entreprises de la même branche de l'économie, contrairement à l'agence de renseignements commerciaux, peuvent compter sur cette défense. Souvent une société en renseigne une autre sur ses rapports avec un client ; le privilège embrasse ces communications si elles ne sont pas entachées d'intentions délictueuses.

Bref, la notion de diffamation demeurera peut-être une voie d'accès à la protection de la vie privée. D'autre part, la différence conceptuelle entre réputation et intégrité de la personne est de nature à restreindre le recours en diffamation pour protéger le caractère privé de l'information personnelle. La réputation se fonde essentiellement sur le jugement et l'estime d'autrui. L'intégrité de la personne, d'autre part, est liée au *moi* du sujet, à l'estime de soi-même. En droit, une fausseté peut être préjudiciable à la réputation. Mais, pour que l'intégrité de la personne soit atteinte, il faut que certains faits échappent à la maîtrise du sujet. L'atteinte à la vie privée n'est donc pas nécessairement diffamatoire, et la diffamation, bien que source d'angoisse, ne viole pas nécessairement l'intimité.

Notons que la diffamation relève aussi du code pénal au Canada. Toutefois la véracité des faits n'y entre pas comme moyen de défense, contrairement à ce qui est prévu pour le délit civil (tort). Par exemple, si une agence de renseignements commerciaux

communiquait un rapport défavorable sur une personne recherchant du crédit, celle-ci pourrait, en principe, poursuivre l'agence en raison du préjudice subi, la partie trouvée coupable serait passible de deux ans de prison. Par contre, la jurisprudence a établi que même si le rapport est faux, l'employé de l'agence ne serait pas tenu responsable de l'acte diffamatoire pourvu qu'il n'ait pas eu pour mobile l'intention de nuire (ill-will), que sa conduite ait été raisonnable dans les circonstances et que la personne ayant reçu le rapport y eût droit.

Par la communication ou l'échange de renseignements, il s'établit, au cours d'une existence, des relations diverses avec autrui. La société et le droit considèrent ces renseignements comme confidentiels en certains cas. Aussi la loi établit-elle une sorte de mur protecteur autour des éléments d'information, les réservant aux intéressés.

À l'occasion des témoignages devant les tribunaux, la question des renseignements confidentiels se pose souvent. Aux termes des lois fédérales et provinciales de la preuve, les entretiens entre mari et femme, entre procureur et client, font l'objet d'un privilège : la divulgation alors n'est pas obligatoire. Diverses lois provinciales protègent d'autres rapports d'une façon analogue. En outre, des informations obtenues par la *Couronne* pourront demeurer confidentielles, si le juge estime que tel est l'intérêt public.

La loi protège aussi le caractère confidentiel par la liberté contractuelle. Ainsi, la personne peut garantir sa vie privée en faisant du caractère confidentiel une condition du contrat. Par exemple, telle personne endettée, contrainte à vendre sa maison, peut stipuler que ce fait sera maintenu secret sous peine de violation du contrat. Le domaine confidentiel dans le contrat peut être aussi étendu que les parties en conviennent.

Les tribunaux se sont montrés enclins, au delà de la relation contractuelle explicite, à voir dans certaines situations un contrat ou une obligation implicites de discrétion. Dès 1888, dans l'affaire *Pollard c. Photographic Co.*[11], un photographe s'est vu empêcher de vendre ou d'exposer des photographies d'une dame prises à la demande de celle-ci moyennant rétribution ; d'une part, un contrat implicite lui aurait interdit de se servir des négatifs à pareilles fins, et, d'autre part, il aurait abusé du pouvoir qu'on lui aurait confié afin de satisfaire un client. Ce raisonnement s'appliquerait tout aussi bien aux situations où telle personne fournit des renseignements à une autre à une fin donnée et où ces renseignements sont ensuite communiqués à des tiers à d'autres fins.

Mais la juridiction d'équité des cours de *Common law* assure

une plus grande protection. Lorsqu'il existe une relation confidentielle, les tribunaux interviendront pour empêcher qu'une partie en abuse. Le caractère confidentiel de la relation peut avoir diverses origines : l'état (par exemple, entre mari et femme); le contrat (par exemple, entre médecin et malade); la législation (par exemple, les lois fédérale et provinciales de l'impôt sur le revenu). Au reste, les tribunaux ont même tenté de protéger des relations confidentielles en dehors des trois conditions ci-dessus. Ainsi, dans l'affaire *Saltman Engineering Co. Ltd. c. Campbell Engineering Ltd.*,[12] qui s'est déroulée en Angleterre en 1948, la compagnie défenderesse avait fabriqué certains outils à son usage d'après des épures fournies à titre confidentiel par la compagnie demanderesse, d'où violation de foi, bien que les deux parties n'eussent pas conclu de contrat. L'un des juges, lord Greene, formula le principe ci-après :

> « L'obligation de respecter le caractère confidentiel ne se limite pas aux cas de rapport contractuel entre les parties... S'il est établi que tel défendeur a exploité directement ou indirectement des informations obtenues de tel demandeur sans le consentement explicite ou implicite de celui-ci, le premier sera tenu coupable de violation des droits du second[13]. »

L'aptitude du droit à évoluer en ce domaine ressort de l'affaire *Argyll c. Argyll*[14], entendue en Angleterre en 1965; le tribunal accorda aux entretiens entre mari et femme une protection dépassant l'usage établi; en effet, la demanderesse obtenait alors un décret interdisant à son ancien époux de publier des faits relatifs à leur vie commune antérieure. Le tribunal fit bien comprendre qu'il ne s'appuyait pas que sur des précédents pour sa décision, mais sur l'esprit de la loi.

« S'il s'agissait d'un cas de jurisprudence bien établie, des indications et des critères faciliteraient sûrement l'exercice de la juridiction à la cour. Si toutefois il existe des communications qui doivent être protégées — ou du moins si tel est l'esprit de la loi — au point de servir de fondement à la règle ancienne voulant que le mari et la femme ne soient pas aptes à témoigner l'un contre l'autre, le tribunal ne doit pas se sentir impuissant parce qu'il ne dispose pas de tout l'arsenal des décisions judiciaires, soit les principes, les règles, les critères, les définitions. Il suffit que le tribunal considère les communications comme confidentielles et leur publication comme élément du préjudice que la loi tend à prévenir sans qu'il lui incombe de définir de nouveau le champ et les limites de sa juridiction : je n'hésite donc pas à conclure que la

publication de certains passages faisant l'objet de la plainte constituerait une violation de la foi conjugale[15] ».

Les deux causes citées sont anglaises, certes, mais des principes analogues s'appliquent aux juridictions canadiennes de *Common law*. Le remède qui s'inspire de l'équité prend généralement la forme d'un décret interdisant d'exploiter ou de divulguer d'une façon préjudiciable des informations obtenues sous le couvert de la confidence. Il arrive aussi qu'on adjuge des dommages-intérêts qui s'ajoutent au décret ou s'y substituent. Cette adjudication est peu fréquente, à vrai dire, mais elle pourrait servir à indemniser la victime d'une violation de la vie privée, notamment dans les cas où l'information a été exploitée à d'autres fins que celles prévues lors de la collecte. Au fait, *l'équité* (equity) peut contribuer largement à la protection de la vie privée, car « le tribunal exerçant une juridiction *d'équité* prononcera la violation de foi indépendamment de la *Common law*[16] ».

Les lois imposant la divulgation de renseignements reconnaissent en bien des cas leur caractère confidentiel. La protection la plus rigoureuse en ce domaine serait celle prévue par la Loi sur la statistique[17], qui interdit strictement de communiquer toute information obtenue en vertu de ses dispositions, et de se servir de cette information pour identifier quelqu'un. La loi fédérale de l'impôt sur le revenu interdit également toute communication de renseignements aux personnes qui n'y ont pas droit légalement. Toutefois, ces interdictions ne figurent en général que dans les lois portant révélation de faits particuliers.

D'autre part, il n'existe pas de principes généraux quant à la nature des informations que les gouvernements puissent légalement recueillir. Les atteintes à la vie privée découlant de la collecte de données comporteront des complications, si les faits consignés n'ont pas de rapport avec les fins de la loi — à plus forte raison si elles sont exploitées ultérieurement à d'autres fins. Certaines lois créent des mesures d'assistance sociale, entre autres, dont l'application exige la collecte de renseignements sur les personnes. Le serment que comporte l'admission dans la fonction publique et la législation générale régissant la violation de foi peuvent sans doute prévenir la communication de renseignements, mais la loi n'offre pas de moyens d'en empêcher l'accumulation. Et sauf en ce qui a trait à l'information délicate, il ne semble pas que soient suffisantes les règles déterminant dans quelles circonstances et à quelles conditions l'information personnelle peut être communiquée dans la fonction publique. Les considérations qui précèdent valent encore davantage dans le cas des entreprises privées, telles les

agences de renseignements commerciaux, car bien des règles en vigueur au gouvernement ne s'appliquent pas à elles.

Outre la diffamation et la violation de foi, la négligence et le principe énoncé dans l'affaire *Wilkinson c. Downton*[19], à l'occasion, donneraient lieu aussi à des garanties quant au caractère privé de l'information.

Si la négligence peut être invoquée relativement aux systèmes d'information et à la vie privée, c'est qu'elle permet le recours le plus général dans le droit actuel concernant les délits civils. Pour que le principe s'applique, il faut que le tribunal statue qu'il existe une obligation de soin et que l'insouciance ou l'incompétence ont été cause de préjudice. Peut-être s'appliquerait-il au cas d'une banque d'information qui, par négligence, n'empêcherait pas la diffusion de renseignements de nature à nuire à la personne qu'ils concernent.

De même le délit de fausse déclaration par négligence pourrait embrasser davantage. Il pourrait comprendre notamment le fait d'une banque indiquant une cote de solvabilité erronée au sujet d'un client, qui plus tard fera faillite. La personne ainsi amenée à lui accorder du crédit aura possibilité de recours. Cet avantage n'a toutefois bénéficié jusqu'ici qu'aux personnes ayant subi des préjudices après avoir pris des décisions fondées sur des renseignements erronés[20]. La portée du recours n'a pas été étendue à la situation opposée, soit celle où le client aurait été lésé, mais cette modification pourrait être apportée éventuellement.

Une possibilité plus lointaine correspond au principe énoncé dans l'affaire *Wilkinson c. Downton* où le tribunal a jugé que la responsabilité d'un préjudice est imputable pour tout acte intentionnel ayant occasionné un dommage matériel. Peu souvent invoqué, ce principe pourrait tout de même trouver quelque application touchant des activités qui se rattachent à la collecte et à la diffusion de l'information. Il a été appliqué dans la cause de *Janvier c. Sweeney*[21], où les défendeurs, des détectives privés, avaient cherché à obtenir des renseignements sur l'employeur de la demandresse en menaçant celle-ci de divulguer des renseignements propres à nuire à son fiancé. La demandresse, ayant subi un choc nerveux, réclama des dommages-intérêts et eut gain de cause.

4. Droit de propriété

Nous avons vu plus haut que le droit peut s'interpréter comme tenant compte de certaines sphères de vie privée relativement aux biens et à la personne physique de l'individu. Certaines protections de la vie privée en matière de propriété ont également de l'importance en ce qui concerne la collecte, le traitement et la transmission de renseignements. La protection de la vie privée sous l'angle de la propriété suggère l'idée d'une sphère d'intimité.

La sphère matérielle de la vie privée a été définie, par le passé, en fonction du droit de propriété. Les garanties juridiques de la jouissance de la propriété résident dans les prescriptions touchant l'intrusion (trespass) et le trouble de jouissance (nuisance) en *Common law*, dans les articles sur le délit en droit québécois et dans certaines dispositions du droit criminel.

La présence physique sur une propriété, si elle est illicite, peut donner lieu à une poursuite en intrusion. Celle-ci, théoriquement, ne nécessite pas la preuve de dommages consécutifs. La seule présence justifie le recours. Les tribunaux, il est vrai, n'adjugeront que des dommages-intérêts symboliques pour des dérangements sans importance, mais il en sera autrement d'une intrusion plus grave. La vie privée est en outre garantie par les dispositions du Code criminel interdisant diverses façons de s'introduire dans une maison ou sur un terrain, telles la violation de domicile et l'intrusion nocturne, infractions qui sont punissables. Ainsi se trouve délimité un espace matériel de vie privée protégeant l'individu.

La législation sur l'intrusion protège le caractère privé de l'information en éloignant physiquement les personnes des sources de renseignement, mais elle n'embrasse pas toutes les intrusions en ce domaine. Ainsi, un intrus découvre dans une maison des faits que le propriétaire estime privés, telle l'appartenance à un parti politique attestée par une carte de membre; une atteinte à la vie privée en résulte, mais elle n'est pas visée par la loi. Mais cela n'exclut pas évidemment les autres recours, dont les poursuites pour appropriation illicite ou vol, si l'intrus a pris la carte. D'autre part, les principes d'équité, des dommages-intérêts accrus et des poursuites au criminel constitueraient sans doute le recours indiqué en cas d'immixtion dans la vie privée d'ordre moral. Il y a aussi des cas où des garanties légales du caractère privé dans l'ordre matériel débordent la propriété et embrassent l'information. Ainsi les lois fédérales et provinciales, exemples bien connus, assurent le secret du scrutin par l'isoloir.

Pour ce qui est des lois régissant la perquisition, une affaire récente au Nouveau-Brunswick, soit celle de *K. C. Irving Ltd. c. la Reine*[22], a fait ressortir la pertinence des considérations sur la vie privée qui embrassent, au delà de la propriété, le domaine de l'information. Dans cette affaire, des préposés aux enquêtes sur les coalitions commerciales avaient, en vertu de mandats en bonne et due forme, effectué des perquisitions chez trois particuliers; ils étaient à la recherche de certains renseignements en rapport avec une accusation en la matière. Le tribunal a conclu que l'émission et l'exécution de ces mandats constituaient des atteintes à la vie privée, car ils avaient été délivrés sans qu'on ait été raisonnablement fondé à croire que les particuliers en question cachaient des éléments de preuve. De même les lois relatives à la fouille de personnes protègent la vie privée. En vertu du Code criminel, la fouille d'une personne ne peut être effectuée que par un agent de police et en certaines circonstances, soit lorsqu'il est fondé à croire que l'individu a commis ou est sur le point de commettre une infraction. Sans quoi, la faute est punissable comme pour quiconque d'autre. Dans la mesure où les voies de fait comportent affront et préjudice physique, la loi protège la vie privée dans l'acception morale comme physique.

Diverses parties de la législation démontrent que les tribunaux font droit aux revendications touchant la vie privée. Depuis nombre d'années, la *Common law* reconnaît à l'individu des droits sur son nom, à son portrait et au contenu de ses lettres personnelles.

L'affaire *Williams c. Settle*[23] illustre bien l'esprit de la loi. Les services du défendeur, photographe commercial, avaient été retenus pour le mariage du demandeur. Un peu plus tard, le beau-père du demandeur était assassiné. Deux journaux persuadèrent le photographe de leur vendre une photographie de la noce, et la publièrent. Williams intenta des poursuites, invoquant que les droits de reproduction de la photographie lui appartenaient. Il n'aurait pas eu gain de cause, il est vrai, si ces droits avaient appartenu au photographe; cependant, comme nous l'avons vu à propos de l'affaire Pollard, les tribunaux sont capables d'ingéniosité pour fonder un recours. Dans l'affaire *Williams c. Settle*, il adjugea des dommages-intérêts exemplaires en raison de l'atteinte aux valeurs personnelles. Le juge Sellers déclara :

> Il suffit de dire qu'il y a eu atteinte flagrante au droit du demandeur, conduite scandaleuse et mépris total non seulement des droits de reproduction du demandeur mais de ses sentiments et de son sens de la dignité familiale. Il s'agit d'une intrusion dans la vie privée d'un individu

plus profonde et plus grave que la violation d'une propriété[24].

Il se peut qu'à partir de causes semblables à celle-ci, réparties dans divers domaines de la jurisprudence, les tribunaux élaborent un recours général pour la protection de la vie privée, mais il n'y a là rien de certain encore.

5. Recours prévus par la législation en cas d'atteinte à la vie privée

Deux provinces ont décidé de ne pas attendre l'évolution des doctrines pour protéger la vie privée par l'entremise des tribunaux ; elles ont adopté des lois promulguant le droit à la vie privée.

La Colombie-Britannique, ouvrant la voie, a adopté en 1968[25] le *Privacy Act*. En vertu de cette loi, les actes qui suivent sont des délits donnant matière à des poursuites sans nécessité de preuves de préjudice : « violer délibérément la vie privée d'autrui sans aucun titre à cet effet » (art. 2), ou se servir du nom d'une personne ou de son portrait (de son identité ou de sa caricature), sans son consentement, à des fins commerciales. Ci-après l'alinéa 2 de l'article 2 :

> La nature et le degré de la vie privée auxquels une personne a droit dans une situation donnée ou relativement à toute question sont fonction de ce qui est raisonnable dans les circonstances, eu égard aux intérêts légitimes d'autrui ; pour déterminer si l'acte ou la conduite d'une personne constituent une violation de la vie privée d'une autre, on prendra en considération la nature, les conséquences et l'occasion de cet acte ou de cette conduite, ainsi que du rapport entre les parties, familial ou autres ».

Jusqu'ici, l'article 2[26] n'a donné lieu qu'à une seule poursuite ; le demandeur, constatant qu'il était surveillé et suivi, tomba malade. Le tribunal de première instance statua que cette surveillance constituait un délit pouvant donner lieu à une poursuite en vertu de la loi. Toutefois le tribunal d'appel jugea que le défendeur n'avait pas enfreint la loi, étant donné que la surveillance était « raisonnable » et que l'inquiétude, l'appréhension et le bouleversement du demandeur étaient sans rapport avec la question de savoir si sa vie privée avait été violée.

Le Manitoba aussi a une loi sur la vie privée, qui est en vigueur depuis 1970[27]. Comme celle de la Colombie-Britannique, mais d'un libellé dont il convient de noter la différence, cette loi fait

un délit, susceptible de poursuites sans preuves de préjudice, de l'acte consistant à violer « sensiblement, déraisonnablement et sans titre » la vie privée d'autrui (art. 2). L'article 3 indique des exemples, dont la surveillance en général, l'interception de conversations téléphoniques, l'exploitation non autorisée d'un nom, l'imitation de la voix à des fins lucratives et l'utilisation non autorisée de documents personnels. Il semblerait, d'après ces exemples, que cette loi fera plus pour la protection de l'individu que celle de la Colombie-Britannique. Ni l'une ni l'autre toutefois ne définit la vie privée, sauf d'une façon négative.

Ces deux lois ont pour objet, semble-t-il, de décourager l'emploi de méthodes de collecte douteuses et les exploitations non autorisées de l'information par les media. D'autres législations provinciales, en particulier au Manitoba, en Saskatchewan et au Québec, se rattacheraient davantage aux problèmes dont le Groupe d'étude se préoccupe.

Le *Personal Investigations Act*, adopté par le Manitoba en 1971, constitue sans doute la législation la plus radicale en matière d'information de caractère privé[28]. Sous réserve d'exceptions importantes en faveur des gouvernements et des administrations municipales, ainsi que de leurs organismes, cette loi renferme les stipulations ci-après : que la personne faisant l'objet des investigations donne son consentement ou en soit avisée par écrit ; que soient exclus certains types d'information (appartenance ethnique, casier judiciaire, données d'enquête non corroborées) ; qu'on s'abstienne de divulguer les données d'un dossier personnel, sauf en certaines circonstances particulières ; que la personne sur laquelle porte le dossier soit autorisée à le voir et soit renseignée sur la provenance de son contenu ; que cette personne puisse en contester les inexactitudes. Il s'agit d'une loi pénale qui, par conséquent, ne crée pas de responsabilité civile, sauf intention délictueuse ou négligence.

Au Québec, les articles 43 à 46 de la Loi de la protection du consommateur (1972)[29] apportent soutien aux personnes faisant l'objet de rapports de solvabilité ; elle les met à même de voir et de se procurer ceux qui les concernent et d'y inscrire leurs observations. Elle ne comporte toutefois aucune restriction quant aux types d'informations qui peuvent être recueillies ou à l'usage qu'on peut en faire. Elle ne fournit non plus aucun moyen de s'assurer que les corrections ont été communiquées aux personnes qui auraient reçu un rapport erroné.

La loi québécoise sur la protection du citoyen (1968)[30]

pourrait être utile dans les cas d'atteinte à la vie privée par un fonctionnaire. L'article 13 se lit ainsi :

> « Le protecteur du citoyen fait enquête à la demande de toute personne chaque fois qu'il a raison de croire que dans l'exercice d'une fonction administrative le titulaire d'une fonction, ... relevant du gouvernement ... a lésé cette personne. »

D'autres dispositions protègent le caractère confidentiel des informations que le protecteur du citoyen aura exigées dans l'exercice de ses fonctions ; les tribunaux notamment ne sauraient le contraindre à les communiquer.

Enfin, la Saskatchewan a adopté en 1972 une loi réglementant les agences de renseignements commerciaux. Le *Credit Reporting Agencies Act*[31] qui doit entrer en vigueur en 1973, rend la licence obligatoire et en détermine les conditions d'obtention et de renouvellement. Ainsi l'agence est tenue à des règles relatives à la communication de renseignements, au contenu des rapports personnels, à la révélation à l'individu des informations le concernant, à l'enregistrement de son désaccord le cas échéant. De plus, elle prévoit, contrairement à la législation du Québec, l'obligation de rendre compte de ce désaccord à ceux qui ont reçu le rapport. Tout comme le *Personal Investigations Act* du Manitoba, cette loi est pénale.

6. Élaboration du droit à la vie privée

Nous venons de voir que le droit canadien relatif à la vie privée accuse certaines lacunes. Il arrive qu'il ne couvre pas certaines situations où le citoyen estime avoir besoin de garanties contre l'intrusion ; parfois aussi la protection qu'il stipule est insuffisante du fait de conditions qui compromettent la portée et l'application des lois. Cependant certains progrès importants sont à signaler.

Parmi les provinces de *Common law*, la Colombie-Britannique et le Manitoba ont adopté des lois faisant de la violation de la vie privée un délit particulier. En matière de jurisprudence, des arrêts de *Common law* laissent entrevoir une certaine sensibilisation aux questions de vie privée se posant en divers domaines, notamment en rapport avec la diffamation et le caractère confidentiel. D'autre part, il n'existe pas encore, en *Common law*, de délit général de violation de la vie privée. La reconnaissance de la notion de vie

privée par les tribunaux ne s'est manifestée que sporadiquement, et uniquement à l'occasion de recours en violations rattachables à d'autres domaines du droit.

Ainsi les influences réciproques des assemblées législatives et des tribunaux devraient tendre à accroître la protection de la vie privée dans les provinces de *Common law*, car ce bien et les valeurs connexes sont mis à l'épreuve par l'efficacité croissante de systèmes d'information comportant des données personnelles. Mais il n'est pas sûr qu'il s'élaborera par l'intermédiaire des tribunaux un délit spécifique contre la vie privée, bien que les lois promulguées par la Colombie-Britannique et le Manitoba jouent en ce sens.

Au Québec, l'article 1053 du Code civil, axé sur la notion de faute, a permis plus de progrès. De fait, l'affaire *Robbins c. la Société Radio-Canada*[32], jugée aux termes de l'article 1053, a fait ressortir, selon certains, que le droit de la vie privée existe au Québec. De plus, la doctrine juridique française, qui pourrait valoir au Québec, tendrait à démontrer que ce droit est assimilable au *droit de personnalité* prévu par le droit civil.

Il serait possible au gouvernement fédéral également de protéger la vie privée grâce à sa compétence en matière de droit criminel. D'une manière générale, il ne l'a pas fait, mais le projet de loi concernant la protection de la vie privée montre son intérêt pour la question.

Quelque conception qu'on ait de la jurisprudence actuelle, il est manifeste qu'elle ne renferme pas de concept général de vie privée, notamment en matière d'information, qui puisse éclairer les décisions des tribunaux et la législation. Tout au plus, le droit canadien débouche sur des conceptions négatives de la vie privée, sur ce qui la contrarie ou y porte atteinte, mais n'engendre aucune vue d'ensemble sur cette question. Des idées sont semées çà et là dans les arrêts des tribunaux et les lois, mais il est loin d'être sûr qu'elles finiront par produire une conception cohérente de la vie privée.

Le Groupe d'étude estime qu'il s'en forme une actuellement en matière d'information et que sa consécration en droit serait socialement avantageuse. Celle-ci pourrait éclairer les arrêts futurs des tribunaux, rendre la législation plus efficace et, d'une manière générale, favoriser une meilleure compréhension des questions en jeu.

Théoriquement, on pourra soutenir que dans notre société tout fait concernant un individu se rapporte directement à sa personnalité et qu'il a donc intérêt, fondamentalement et en permanence, à ce que ces faits ne soient pas communiqués à son insu ou contre son

gré. La société peut intervenir de diverses façons et pour diverses raisons et exiger que l'individu divulgue certains faits, mais alors elle doit attacher à la vie privée l'attention qui lui est due.

Peut-être une sphère d'intimité doit-elle être à l'abri de toute intrusion pour que la personnalité essentielle de l'individu ne soit pas violée, bien que ses limites puissent être légitimement modifiées par des décisions judiciaires ou législatives répondant à d'autres besoins sociaux. Cette considération vaut, que l'individu ait ou non connaissance des intrusions. Une fois reconnu le droit à cette sphère, on pourrait en envisager les limites légales. Alors il faudrait mettre en balance les intérêts de l'individu et les autres intérêts de la société, puis examiner si certains types particuliers de renseignements sont à protéger. Cette catégorie serait peu considérable – et restreinte selon certains, à l'appartenance religieuse, à l'origine ethnique, aux opinions politiques et au comportement sexuel. Il faudrait évidemment bien peser les avantages découlant des banques d'information et en outre examiner la question de la communication et de la diffusion ultérieure des diverses catégories d'information. Le droit à la vie privée en matière d'information serait reconnu en principe par la société et sanctionné par la loi. Il resterait à déterminer par la législation, les voies judiciaires puis la réflexion socio-politique, les limites de ce droit.

Théoriquement, la notion de sphère d'intimité est dans la ligne de la tradition du libéralisme socio-politique qui a déjà reconnu et défini d'autres droits découlant de la personnalité, telle la liberté de parole, de culte et d'assemblée. Mais on peut aussi y voir un aboutissement, car elle exempte l'individu de l'obligation de proclamer ses droits pour se livrer librement à des activités particulières (parole, culte et assemblée). En affirmant son droit à la vie privée, peut-être exige-t-il simplement qu'on le « laisse tranquille », comme disaient Warren et Brandeis, et libre d'agir à sa guise dans les limites de la loi. Dans cette perspective, la gamme des droits déjà reconnus atteindrait son élargissement logique ; elle embrasserait les libertés déjà mentionnées ainsi que les droits découlant de la personnalité.

Juridiquement, l'élaboration de ce droit pourrait bien être le fait de la jurisprudence, ou encore de législations par les diverses autorités compétentes. À cet égard, les lois adoptées par la Colombie-Britannique et le Manitoba sont des plus significatives, bien qu'elles contribuent peu à définir le droit à la vie privée ou à le situer par rapport aux autres besoins sociaux. Le travail de la Commission pour l'uniformité de la législation et celui des autres groupes d'étude des provinces de *Common law* incitent à croire

qu'il s'agit là d'une œuvre de précurseurs et qu'une législation plus considérable est à prévoir.

Au Québec, l'Office de révision du Code civil a déjà proposé une charte des droits qui confirmerait, à son avis, le droit à la vie privée sans qu'il soit nécessaire de promulguer une loi nouvelle. En proposant cette charte, l'Office a déclaré s'être fondé sur l'article 12 de la Déclaration universelle des droits de l'homme, qui avait commencé à s'appliquer dans la jurisprudence du Québec. Cet article est conçu comme il suit :

> Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou atteintes.

La Déclaration canadienne des droits, à l'échelon fédéral, apparaît à certains comme propre à embrasser le droit à la vie privée. Mais il faudrait établir ce point avec précaution, compte tenu de divers facteurs, dont la valeur et l'applicabilité de ce droit de création fédérale au Canada.

De toute façon, que soient promulguées ou non des lois sur la vie privée et quelle qu'y soit la précision du ou des concepts de la vie privée, il appartiendra surtout aux tribunaux de déterminer si les revendications à ce titre dans les cas particuliers doivent être acceptées et de délimiter la sphère d'intimité relativement aux autres besoins sociaux. Il pourrait découler de cette approche directe une législation plus cohérente.

De plus, un concept cohérent de droit à la vie privée serait propre à sensibiliser les juges, les législateurs, les fonctionnaires et les administrateurs d'entreprises aux revendications d'une vie individuelle face à l'information, et à mettre en lumière ce qu'on réclame. Enfin, en s'imposant dans les délibérations sociales et politiques sérieuses, il inspirerait les particuliers soucieux de faire incorporer le droit à la vie privée dans la loi.

7. Pour des mesures suffisantes

Même si le droit à la vie privée était bien établi en droit canadien, dans quelle mesure, d'après les recherches du Groupe d'étude, les tribunaux peuvent-ils contribuer à résoudre les problèmes que posent ou pourront poser les systèmes d'information ? Le Groupe d'étude estime que seuls ils ne peuvent qu'apporter des solutions partielles.

C'est que la vie privée n'est pas la seule valeur qui soit mise en

jeu par le développement et l'exploitation croissante des systèmes d'information, ainsi qu'il ressort de nos recherches. Il faut notamment empêcher la diffusion de données préjudiciables, assurer l'accès des données à ceux qu'elles concernent et régler la question de l'exactitude. L'État doit en outre faire valoir les besoins de l'individu face aux vastes systèmes d'information automatisés des grandes organisations. Il serait peu utile sinon tout à fait vain de chercher à tenir compte de ces intérêts ou de ces revendications en se limitant au point de vue judiciaire.

La nature des voies judiciaires explique aussi que des solutions axées sur les tribunaux peuvent être insuffisantes. Il y aurait divers inconvénients à s'en remettre aux tribunaux pour qu'ils élaborent des principes de *Common law* ou interprètent des dispositions législatives. Les litiges coûtent cher et exigent beaucoup de temps parfois ; l'élaboration de principes est lente et s'effectue cause par cause, même lorsque des lois ont été promulguées ; les citoyens qui ont la possibilité de recourir aux tribunaux ne sont pas nécessairement représentatifs des groupes sociaux les plus fréquemment victimes de violations de la vie privée ; il se peut que les tribunaux ne possèdent pas toute la compétence qu'exigerait une technologie informatique en rapide évolution ; le recours à la justice tendra à se limiter aux situations comportant des considérations pécuniaires importantes, alors que de graves atteintes à la vie privée sans répercussions d'argent immédiates peuvent n'être jamais portées devant les tribunaux ; règle générale, la justice vise la réparation de dommages définis. Les violations de la vie privée peuvent être constantes, simplement contrariantes et mineures dans bien des cas, et souvent se produire sans que l'individu en soit conscient. Il faut donc exercer un contrôle incessant sur les systèmes d'information afin de prévenir ces atteintes, de compléter les voies judiciaires se limitant à la réparation des préjudices.

Finalement, il faudrait ajouter aux réparations que peut assurer la justice des conceptions plus progressives et plus souples, et faire la part de ce qu'exigent mise en œuvre et utilisation des ordinateurs selon leurs fins propres. Cette manière de procéder se rattacherait davantage au domaine administratif et réglementaire qu'à celui de la loi et de la justice. C'est justement là le point que nous allons aborder dans les pages qui suivent.

1. WARREN et BRANDEIS, *The Right to Privacy,* 4 Harvard Law Review, p. 193

2. POUND, Roscoe ; *Interests of Persanality* (1915), 28 Harvard Law Review, p. 343.

3. S.O. 1965, chap. 102 ; R.S.O. 1970, chap. 362.

4. Loi sur la radio, S.R.C. 1970, chap. R-1.

5. Loi incorporant la compagnie de téléphone Bell du Canada S.C. 1880, ch. 67, art. 25.

6. Bill C-6, projet de loi sur la protection de la vie privée.

7. Code criminel, S.R.C. 1970, chap. C-34.

8. Privacy Act, S.B.C., 1968, chap. 39 ; Privacy Act, S.M., 1970, chap. 74. Voir également *Davis c. McArthur* (1970), 72 W.W.R. 69, 10 D.L.R. (3d) 250 ; portée en appel en 1970, 17 D.L.R. (3d) 760.

9. *Robbins c. Canadian Broadcasting Corporation* (1958), 12 D.L.R. (2d) 35.

10. *Green c. Minnes* (1891), 22 Ont. R. 177.

11. *Pollard c. Photographic Co.* (1888), 40 ch. D. 345.

12. *Saltman Engineering Co. Ltd. c. Campbell Engineering Co. Ltd. (1963),* 3 All E.R. 413 n.

13. *Ibidem,* p. 414.

14. Argyll c. Argyll (1965), 1 All E.R.

15. *Ibidem,* p. 625.

16. *Ibidem,* p. 619.

17. Loi sur la statistique, S.R.C. 1970, chap. S-16.

18. Loi de l'impôt sur le revenu, S.C. 1970-1971, chap. 63, art. 241.

19. [1897] 2 Q.B. 57.

20. E.q. *Hedley-Byrne c. Heller* (1964), A.C. 465 ; *Minister of Housing and Local Government c. Sharp* (1970) 1 All E.R. 1009(C.A.) ; *Dutton c. Bognor Regis U. D. C.* (1972) 2 W.L.R. 279 (C.A.).

21. [1919] 2 K.B. 316.

22. Voir *K. C. Irving Ltd. c. The Queen,* (1971) 4 C.P.R. (2d) 120.

23. *Williams c. Settler* (1960), 2 All E.R. 806.

24. *Ibidem,* p. 812.

25. S.B.C. 1968, chap. 39.

26. *Davis c. McArthur,* (voir note 8).

27. S.M. 1970, chap. 74, modifié S.M. 1971, chap. 82.

28. Manitoba Personal Investigations Act, S.M. 1971, chap. 23.

29. Loi de la protection du consommateur, S.Q. 1971, chap. 74.

30. Loi du protecteur du citoyen, S.Q. 1968, chap. 11.

31. S. Sask. 1972, chap. 23.

32. (1958), 12 D.L.R. (2d) 35.

Chapitre 12
Solutions d'ordre réglementaire

1. Introduction

La réglementation des systèmes d'information a fait l'objet de diverses propositions tendant à protéger la vie privée et les valeurs connexes peut-être en danger. Certaines ont été présentées directement au Groupe d'étude tandis que d'autres étaient exprimées dans les ouvrages et les articles sur le sujet, ou encore dans les rapports d'organismes d'autres pays œuvrant dans le même domaine. Il s'agit de propositions d'ordre réglementaire puisqu'elles visent les activités des banques d'information ; elles tendent à faire interdire certaines pratiques considérées comme portant atteinte à la vie privée et aux valeurs connexes, ainsi qu'à faciliter aux particuliers l'accès aux dossiers personnels les concernant, eu égard toutefois au bon fonctionnement des banques d'information. L'autoréglementation mise à part, ces propositions comportent des prescriptions plus ou moins détaillées, qui seraient énoncées dans des lois ou des règlements, et appliquées sous la surveillance d'un mécanisme administratif. Le recours aux tribunaux y est envisagé.

Presque toutes les autorités en la matière – et tout récemment le *Younger Committee on Privacy*, de Grande-Bretagne, et Arthur

Miller dans *Assault on Privacy (1971)* – ont préconisé une certaine réglementation ou, au minimum, un contrôle constant des opérations des banques d'information dans la mesure où elles attentent à la vie privée et aux valeurs connexes [1]. La *British Computer Society* a consacré une vaste étude à l'autoréglementation.

Aussi l'objet du présent chapitre est-il d'exposer et d'analyser les diverses propositions tendant à réglementer les banques d'information et les pratiques en ce domaine en vue de sauvegarder les droits de l'individu. Plusieurs de ces propositions sont déjà incorporées à des lois provinciales, notamment à la Loi de la protection du consommateur (Québec), au *Personal Investigations Act* (Manitoba), et au *Credit Reporting Agencies Act* (Saskatchewan). Nous examinerons en outre les propositions ou législations d'autres pays.

Dans des chapitres antérieurs, la vie privée face à l'information a été qualifiée de « sphère d'intimité ». Dans la pratique, cet aspect de la vie privée ne fait pas l'objet d'une protection suffisante. Si les causes relatives à la vie privée ont été jugées selon l'esprit des recours existants, l'absence de moyens de droit généraux en cas de violation pose toujours un problème. Il existe peu de lois délimitant les données personnelles que les systèmes d'information peuvent recueillir et stocker, ou prescrivant qui peut accumuler des données personnelles et constituer des dossiers sur les particuliers, ou qui peut avoir accès à ceux-ci. La réglementation des usages en la matière peut sauvegarder la vie privée et les autres intérêts du même ordre.

Il importe de ne pas perdre de vue, en étudiant les propositions en cause, qu'elles tendent à réglementer les usages de systèmes d'information dont dépendent de plus en plus nombre de secteurs de la société. Dans ces systèmes, les faits sont traités et « livrés » aux fins des connaissances que nécessitent les décisions appropriées, qu'il s'agisse de déterminer l'espace disponible pour tel vol ou de consigner quels clients sont en retard dans leurs paiements ou qui a droit aux allocations familiales ou aux prestations d'assurance chômage. Bref, les systèmes d'information permettent aux entreprises, à l'État et aux organisations diverses de tenir compte de leurs propres besoins et de donner satisfaction à la société d'une manière efficace. Ce dernier point est important ; individus et groupes dans une société expriment sans cesse des exigences nouvelles et croissantes que seules peuvent satisfaire des entreprises bien administrées ; mais, celles-ci, de leur côté, doivent se renseigner sur individus et groupes et exploiter cette information. Par conséquent, toute réglementation des banques d'information doit tenir compte

du souci, chez les organismes publics et les entreprises, de recueillir, de traiter et d'utiliser des données pour s'acquitter de leurs tâches et remplir leurs obligations sociales. Pour être efficace, elle doit donc protéger l'individu sans gêner indûment le fonctionnement des systèmes d'information légitimes.

2. Champ de réglementation

Au chapitre 10, les questions de vie privée et de valeurs connexes mises en cause par le processus d'information ont été divisées en cinq catégories en fonction des activités ci-après : collecte des données, contenu des fiches, stockage et traitement des données, diffusion des données et accès à celles-ci. Les possibilités de réglementation dans ces domaines se répartissent selon les mêmes catégories.

a. Collecte des données

La manière dont les organisations recueillent les données peut entraîner des atteintes inutiles à la vie privée ou avoir d'autres effets préjudiciables. Quelques-unes des propositions touchant ce point tendent à restreindre les méthodes employées ; d'autres limiteraient l'emploi de l'information aux fins précises pour lesquelles elle a été recueillie.

Le recours à l'écoute clandestine et à des dispositifs de surveillance a été signalé comme particulièrement indésirable. Le Parlement, qui étudie des projets de loi sur les tables d'écoute, envisage déjà des mesures qui interdiraient l'emploi de ces appareils dans les investigations privées, sauf s'il s'agit de l'application de la loi et de la sécurité de l'État, et qui feraient une infraction de leur possession.

On a proposé, outre ces mesures, qu'il soit interdit de stocker dans des banques d'information des données recueillies clandestinement à l'aide d'appareils électroniques ou mécaniques. Ce serait un moyen de dissuader le personnel de ces banques de pratiquer la collecte subreptice. Comme dans la législation sur les tables d'écoute, des exceptions pourraient être prévues, notamment en faveur de l'application des lois. Le plus gros des données sur les criminels et les suspects est accumulé par des voies indirectes. Ces données, essentielles aux enquêtes de la police, portent sur les procédés, les complices, les lieux d'habitation, etc. En gêner la collecte entraverait l'application de la loi.

D'après la plupart des propositions, il faudrait établir des

lignes directrices touchant les titres des préposés à la collecte, leur conduite et les méthodes à employer.

On a aussi exprimé le vœu que la collecte se limite aux éléments d'information se rattachant aux fins indiquées. Ce moyen, dont on a dit qu'il « restreignait l'enquête directe », aiderait à prévenir la collecte d'informations superflues et à réduire le risque qu'elles soient utilisées à mauvais escient.

Toutefois, restreindre l'enquête directe n'irait pas sans quelques difficultés. Tout d'abord, il n'est pas toujours facile pour le particulier de contester la pertinence d'éléments d'information qu'on exige de lui, s'il doit fournir les renseignements pour recevoir telle prestation, qu'il ait droit à celle-ci (assistance sociale) ou qu'il s'agisse d'une opération commerciale (crédit). Ensuite, beaucoup de gens ont été amenés à se croire obligés de donner les renseignements sollicités ; cependant, les groupes faisant souvent l'objet de recherches (tels les autochtones) et d'enquêtes publiques (telles les entreprises commerciales) ont de plus en plus tendance à demander pourquoi on les interroge. Ainsi, en Colombie-Britannique, une femme de Vancouver a refusé à l'assistance sociale de révéler qui était le père de son enfant illégitime ; la justice a rendu un arrêt en sa faveur, déclarant sans pertinence le renseignement demandé. Restreindre l'enquête directe pourrait accentuer la tendance à mettre en question la collecte de données superflues ou hors du sujet.

Autre problème, la pertinence d'un élément d'information dans une situation donnée est matière hautement subjective. C'est le fait de celui qui recueille l'information et de celui qui en est l'objet, ce qui peut occasionner des confrontations au cours de la collecte. Des directives générales pourraient être utiles, mais elles ne s'appliqueraient qu'à un nombre limité de situations. Les grands établissements qui recueillent des données craignent que pareille façon de procéder, entraînant de graves lacunes dans l'information, compromette le processus des décisions.

Selon une proposition, il conviendrait non seulement de restreindre les enquêtes, mais d'interdire globalement la collecte de certains types de données. Les seules exceptions seraient déterminées par un intérêt social manifeste consacré par la législation, et conformément à des prescriptions contre les abus. Leur énumération n'est pas bien établie ; justement l'un des inconvénients de cette approche est que l'accord est à peu près impossible sur ce point. De toute façon, les opinions politiques, l'appartenance religieuse et le comportement sexuel comptent d'ordinaire parmi les catégories protégées. Il faudrait veiller à ne pas gêner indûment

ni censurer le mouvement de l'information et des connaissances dans la société. C'est que certains pourraient consentir à communiquer des renseignements à l'occasion de sondages ou d'enquêtes par des universitaires, par exemple, mais répugner à faire part des mêmes faits à l'État ou à des entreprises.

b. Le contenu des fiches

Des données peuvent être pleinement utiles au moment de la collecte, puis perdre leur valeur avec le temps. Citons à titre d'exemples les casiers judiciaires, les infortunes financières, les maladies physiques et les écarts de jeunesse. On craint que les ordinateurs, en raison même de leur efficacité, fassent que les erreurs et les mésaventures ne soient jamais oubliées, et en fait jamais pardonnées, dans le processus d'information.

Bon nombre de systèmes d'information ont pour règle de retirer les données désuètes des dossiers sur les personnes, bien qu'aucune loi ne les y oblige. Il est assez fréquent que les contrats entre employeurs et employés renferment des dispositions sur ce point. Des règles générales ont été établies quant à l'élimination des données désuètes, avec des limites de temps précises variant selon la nature de l'information et le type de banque d'information.

L'exactitude des données préoccupe plus que leur pertinence. Quand le crédit, l'assurance ou l'emploi sont en jeu, des informations inexactes peuvent causer de graves préjudices. Les épreuves d'exactitude sont des plus difficiles à définir, car une information peut être vraie en soi mais fausse dans son contexte. Ainsi le non-paiement d'une dette sans la notation de raisons légitimes. On a proposé qu'il soit permis aux individus d'élucider ces points en insérant leur propre version dans le dossier. D'ailleurs le Québec, le Manitoba et la Saskatchewan ont légiféré en ce sens.

L'exactitude est liée aussi aux notions de validité des données. Des dossiers périmés peuvent être exacts quant à leur contenu, mais inexacts à la lumière de faits ultérieurs. Ainsi, dans le cas d'une dette acquittée mais dont le paiement n'est pas consigné avant plusieurs mois, il y aura inexactitude jusqu'à la mise à jour. Comme il incombe au préposé aux données de veiller à l'exactitude des dossiers, il devrait être tenu, a-t-on proposé, à mettre à jour et revoir périodiquement les dossiers.

c. Stockage et manipulation des données

Sous l'angle du stockage, le caractère personnel se ramène au caractère confidentiel, et celui-ci dépend de la sécurité du système. La sécurité des données se mesure à la protection du caractère personnel. Mais sécurité n'est pas, pour autant, synonyme de caractère privé. Les systèmes les plus sûrs, tels ceux de la police et des services de renseignements, peuvent être les plus irrespectueux de la vie privée. Un système peu sûr n'en constitue pas moins un risque supplémentaire, outre tous les autres que le système peut comporter.

Dans le chapitre 9, le Groupe d'étude examine où en est la sécurité des systèmes d'information au Canada et analyse les moyens de l'accroître. Le degré de sécurité nécessaire est déterminé par le caractère plus ou moins délicat du contenu de chaque système et par la valeur des données pour ceux qui pourraient avoir intérêt à y accéder. Les informations financières sont généralement délicates et d'une grande valeur. Quant aux données médicales, elles auraient du prix surtout pour le sujet.

Indépendamment du caractère délicat des informations, la sécurité qui convient varie entre les systèmes selon leur importance, leurs caractéristiques techniques, la valeur des données stockées et les ressources dont on dispose pour la sécurité. Comme les mesures de sécurité ont pour objet de restreindre aux personnes agréées l'accès aux systèmes, et que les systèmes automatisés se prêtent plus facilement aux techniques de protection, l'automatisation permettrait d'établir des normes générales. L'objet principal des cotes sécuritaires serait d'élever le prix de l'intrusion au delà de la valeur – au sens propre ou figuré – des informations convoitées.

Comme souvent l'attention se laisse mobiliser par les mots de passe et les « verrouillages » subtils des systèmes informatiques, par les procédés de codage et par la transmission à distance, on a tendance à oublier un principe essentiel de la sécurité : une chaîne n'est pas plus forte que son anneau le plus faible. Un recenseur bavard, rappelons-le, peut faire plus de tort qu'un mot de passe faux. Nos recherches ont dégagé le cas de données hautement confidentielles transportées, sur bande, par un chauffeur de taxi non accompagné.

Le Groupe d'étude a pris note de diverses propositions voulant que les préposés à la manipulation des données personnelles soient tenus à l'autorisation et à la caution sécuritaires. Les autorisations de cet ordre sont courantes dans certaines sphères de

l'administration publique et de l'entreprise, mais les cotes sécuritaires varient selon le caractère plus ou moins délicat de l'information. Des normes d'application générale ne seraient peut-être pas faciles à établir. La caution est une mesure complémentaire normale en matière de responsabilité civile et serait, pour cette raison, d'une utilité restreinte.

d. Communication des données

C'est la communication de données personnelles individualisables qui fait courir les plus grands risques à la vie privée. Les informations sur un individu recueillies avec son consentement à des fins qu'il approuve peuvent être offertes à d'autres personnes à son insu et servir à des usages qu'il ne connaît ni ne sanctionne. C'est là que l'individu perd la maîtrise d'informations le concernant, que s'avivent ses craintes de n'avoir plus de lieu propre où abriter son passé (immédiat ou éloigné), que sa vie privée est le plus exposée.

Une large gamme de mesures de protection a été proposée. On pourrait assujettir à une restriction globale tout échange de données entre banques d'information. Selon une proposition plus modérée et mieux applicable, on limiterait les échanges à des destinataires qui sont aptes à démontrer le « besoin de savoir » ou qui sont touchés par les fins de l'information recueillie. La communication pourrait aussi être restreinte aux données se rattachant immédiatement à ce besoin. Il y aurait lieu de définir des principes généraux qui régiraient les échanges autorisés.

Diverses propositions portent en outre sur le rapport entre l'individu et la banque d'information. Peut-être faudrait-il rendre obligatoire le consentement de l'individu aux échanges envisagés, ou encore cette solution entraînant des frais considérables, limiter cette condition aux cas où l'information sur lui serait destinée à d'autres fins que celles prévues à l'origine. Suivant une proposition connexe, l'individu consentirait lors de la collecte à une gamme d'échanges prévisibles avec d'autres banques d'information. Enfin, une conception plus souple voudrait que la banque rende compte à l'individu de tous les échanges, ou lui en communique une liste sur demande et lui fournisse la possibilité, quand il le jugerait à propos, de contester tel échange à la lumière des objectifs déclarés de la banque.

Le consentement pose des problèmes complexes. Tout d'abord, on verrait bien des inconvénients à une formule obligeant à

consulter l'individu chaque fois qu'on envisagerait de communiquer des informations. À un autre point de vue, le consentement pourrait parfois être difficile à déterminer. Ainsi, des informations personnelles pourraient être communiquées par un organisme d'assistance sociale – manifestement pour le bien de l'individu. Vraisemblablement, celui-ci ne chercherait pas à empêcher cette diffusion, mais saurait-on si le consentement a été vraiment libre ? En certains cas, l'information aurait été recueillie à une fin déclarée, mais son exploitation à d'autres fins pourrait être d'un avantage insigne pour d'autres personnes et pour la société en général ; songeons ici à l'application de la loi, notamment lorsque la sécurité de l'État est en jeu. Certains estimeront qu'il y a désistement de cette obligation dans ces cas. Toutefois, ils voudront quand même sauvegarder la vie privée. Aussi, a-t-on avancé que les corps policiers demandant accès à des données pourraient bien être soumis à l'obligation du mandat de perquisition, à peu près aux conditions spécifiées dans le Code criminel. De plus, les interdictions actuelles relatives à la divulgation – par exemple, celles qui s'appliquent aux médecins et aux avocats, ou celles qui concernent l'utilisation des dossiers de l'impôt ou des données du recensement – pourraient rester en vigueur[2].

Les contrôles touchant la diffusion des données ne peuvent être embrassés dans une seule formule applicable à tous les cas. Trop rigoureux, ils risqueraient de gêner le fonctionnement des systèmes d'information et de priver les individus de l'accès à une information qui normalement devrait être publique. Tout contrôle ne devrait-il pas tendre à limiter la diffusion aux cas de besoin évident et, si possible, aux cas où le sujet des données aura exprimé son consentement.

e. Accès des personnes aux dossiers les concernant

Selon un thème qui revient souvent dans le rapport, c'est la vie privée de l'individu qui peut être violée, et ce sont les établissements – les banques d'information, plus précisément – qui ont l'occasion d'y porter atteinte. L'inégalité est patente. Et il en est ainsi à toutes les étapes du processus. L'individu aura consenti à donner des renseignements sur lui-même en vue d'un avantage, ou bien l'information sera recueillie à son insu. Le préposé à la banque détermine unilatéralement le degré de sécurité nécessaire. Et, sauf exceptions, il décide si l'information sera diffusée à des tiers.

Ce déséquilibre des pouvoirs entre la personne que concernent les données et celle qui les détient est le motif principal de nombre

de propositions de mesures réglementaires. Or, quoi qu'on fasse pour remédier à ce déséquilibre, par exemple contrôler les activités des banques d'information, il faudrait toujours consulter l'individu. Lui seul peut dire si tels types d'information ont de l'importance pour lui, et par conséquent s'ils valent l'effort nécessaire pour assurer leur exactitude ou limiter leur diffusion. À l'heure actuelle, l'individu n'a guère de moyens de contrôler le mouvement de l'information sur son compte, sauf le recours en justice ou une plainte à son député ou à la presse. Cette lacune tient à ce que l'individu est peu renseigné sur l'usage que l'on fait de l'information le concernant, et partant n'a guère l'occasion de le discuter.

Beaucoup d'auteurs qui ont écrit sur le sujet ont préconisé pour l'individu le droit d'accéder aux informations le concernant. Pour ce qui est du crédit, le *Fair Credit Reporting Act* (1971), aux États-Unis, et les recommandations de la Commission Younger, en Grande-Bretagne, prévoient déjà cet accès.

Fondamentalement, le droit d'accès assurerait à l'individu le droit d'être renseigné sur l'existence de tout dossier renfermant des informations personnelles sur lui et d'en prendre connaissance après demande à cet effet. Dans la plupart des textes, ce droit comporte la faculté de mettre en question un élément du dossier qui ne lui semblerait pas exact, complet, actuel ou pertinent. Les législations du Québec, du Manitoba et de la Saskatchewan accordent à l'individu le droit d'exiger que son propre point de vue soit consigné au dossier, pour qu'il puisse développer ou préciser certaines données qui, autrement, demeureraient vagues ou trompeuses.

La plupart des gens savent, d'une manière générale, s'il existe sur eux des dossiers importants (en matière de finance, de crédit, d'assurance ou de soins médicaux) et où ils se trouvent. Mais, sans doute, ils ne sont pas au courant de tous. Il ne leur est pas fait part, non plus, des changements qui y sont apportés. Aussi a-t-on proposé que les banques d'information avisent les intéressés de la création d'un dossier sur eux ou des changements majeurs apportés aux dossiers existants.

Les notifications peuvent prendre une grande variété de formes. On peut simplement faire savoir à l'individu qu'un dossier sur lui est ouvert et préciser à quelle fin; on peut lui expédier une copie complète ou partielle du dossier, ce qui coûterait 8 ¢ ou 9 ¢ par copie, d'après l'estimation de la Commission Younger; on peut aussi comme complément à l'une ou l'autre des méthodes ci-dessus, aviser l'individu de toute utilisation de son dossier ou lui assurer la possibilité de se procurer un état de ces utilisations.

En faisant un choix, il faudra mettre en balance l'efficacité – qui se traduira par des avantages pour l'individu – et le prix que devront payer les banques d'information. Si les témoignages sur ce point ne sont pas concluants, il ne semble pas que la plupart des particuliers s'estimeraient suffisamment en cause pour rechercher une information complète, c'est-à-dire des copies des dossiers et des avis de toutes les utilisations. Certains, tout de même, tiendront à exercer ces droits. Il suffirait vraisemblablement d'assurer aux individus le droit de se faire remettre une copie complète du dossier tenu par les grands systèmes d'information et d'être renseigné sur toute utilisation de celui-ci, mais il n'y aurait pas lieu de pousser cette politique au point où des masses de renseignements non désirés seraient expédiées par la poste aux individus.

Il convient d'examiner certaines difficultés d'ordre pratique qu'entraînerait le droit général d'accès et de notification sur demande. Certains dossiers, tels ceux des agences de renseignements commerciaux, sont établis en langage codé, alphanumérique. Il faudrait donc les interpréter pour les personnes demandant l'accès aux dossiers. L'accès sera d'une valeur moindre si les banques d'information ont le loisir d'imposer des tarifs exorbitants pour l'exercice de ce droit. Cela se serait produit d'ailleurs : après que le *Fair Credit Reporting Act* eut été adopté aux États-Unis, des frais allant jusqu'à $ 25 auraient été exigés. Et, autre problème, des banques d'information, dit-on, auraient profité de visites à la banque pour recueillir des indications supplémentaires sur l'individu.

Si un droit général d'accès était reconnu, il faudrait manifestement prévoir d'importantes exceptions. Les dossiers médicaux, notamment en psychiatrie, peuvent renfermer des données qu'il est préférable de ne pas laisser voir à l'intéressé. Les dossiers des services de renseignements seraient, il va de soi, des cas d'exception. Les corps policiers pourraient réclamer la même exemption, bien qu'un accès partiel se conçoive pour eux. Les dossiers de base de la police peuvent se répartir en casiers judiciaires et en données d'investigation. Selon une proposition, l'accès pourrait être accordé à la partie des dossiers touchant les actes délictueux, les arrestations, les condamnations et les sentences, qui forment des données « objectives » et font partie des archives publiques. L'accès aux dossiers des infractions est assuré grâce au *U.S. Project Search*, système automatisé d'échange d'information policière entre les États. L'accès aux données d'investigation (dont la manière d'opérer, les complices connus et les lieux d'habitation) ne serait manifestement pas souhaitable.

On a fait valoir que la plupart des gens exerceraient rarement leur droit d'accès, et que les banques d'information qui seraient poursuivies pour dommages résultant d'informations fausses soutiendraient probablement que le non-exercice du droit d'accès implique l'acceptation des données consignées au dossier. Un point de vue opposé voudrait que le droit à l'accès, bien que peu exercé, incite fortement les banques d'information à un plus grand souci d'exactitude ; elles voudraient s'épargner les frais et la perte de temps qu'entraîneraient les litiges avec des particuliers sur des données de détail.

Il est une question qui se rattache à celle de l'accès, soit celle du consentement délibéré ou en connaissance de cause ; elle a longuement retenu, aux États-Unis, l'attention de la *President's Commission on Federal Statistics.* Par « consentement délibéré », termes dont la signification n'est peut-être pas évidente, on entend que les individus doivent savoir exactement pourquoi on se renseigne sur eux et à quels usages sont destinés les renseignements.

3. Objet de la réglementation

Le terme *banque d'information*, comme nous l'avons mentionné plus haut, est une abréviation commode pour désigner divers types de systèmes qui ne sont pas homogènes et qui ne forment pas une catégorie bien définie. Tel système – celui des dossiers médicaux, par exemple – peut présenter des ressemblances matérielles et de fonctionnement avec un système de dossiers financiers, mais l'un et l'autre seront entièrement distincts quant à leur contenu et à leurs objectifs. Ce qu'il s'agit de réglementer, ce ne sont pas les banques d'information en soi, mais les activités des systèmes d'information renfermant des données personnelles dont un mauvais emploi pourrait être cause de préjudices aux individus. Ainsi, le degré de réglementation qui pourrait convenir dans le cas d'une banque d'information renfermant des données très délicates, par exemple celles d'une agence de renseignements commerciaux, serait peu approprié pour une banque d'information renfermant des données accessibles au public comme celles d'un rôle de cotisation municipal.

Malgré le prestige qui s'est attaché au terme, *banque d'information* ne désigne rien d'autre qu'un stock de données dont on peut extraire des éléments à volonté. Ces données peuvent être de toutes sortes, depuis les recettes de cuisine jusqu'aux numéros d'un annuaire téléphonique. L'Organisation de coopération et de développement économiques (O.C.D.E.) s'est employée à mettre au

point une définition précise et opérationnelle de la banque d'information personnelle. Mais la préférence du Groupe d'étude va à celle élaborée par la *Manitoba Law Reform Commission* :

> Opération de stockage d'informations permettant de fournir des données personnelles sur des individus identifiables par leurs noms ou par des moyens grâce auxquels on peut retrouver facilement ces noms.

Cette définition embrasse les systèmes manuels ou automatiques ; d'autre part elle exclut les systèmes statistiques, sauf dans les cas où, pour mettre les données à jour, on tient des dossiers individuels codés. Un projet de loi, dont l'objet était de limiter le nombre des banques d'information en Grande-Bretagne, visait à exclure tous les systèmes ne renfermant pas, au minimum, cent mille noms.

Au début du présent Rapport, nous répartissions les systèmes entre trois catégories : administration, statistique et renseignements. Les systèmes de renseignements, qui forment une catégorie à part pour des raisons de sécurité, ne devraient pas normalement être assujettis à la réglementation générale. Quant aux systèmes administratifs, qui forment la catégorie la plus considérable, et de loin, il convient de les diviser en deux classes : interne (employés) et externe (clients, etc.), puis de subdiviser cette dernière en divers groupes fonctionnels (finance, soins médicaux, etc.).

Il y a lieu aussi de noter deux autres moyens ou formules, qui tendraient à réduire la réglementation aux domaines posant des difficultés. Certains peuvent soutenir qu'une réglementation générale est inappropriée, voire inapplicable étant donné la diversité des types. Elle pourrait plutôt viser des domaines définis, tel celui des dossiers médicaux ainsi que l'a proposé l'*Ontario Medical Association*. Le Québec et la Saskatchewan ont mis en œuvre des mesures analogues dans le domaine du crédit, et l'assemblée législative ontarienne est saisie de cette question.

L'avantage de cette méthode est d'accorder de l'attention aux domaines précis qui en exigent, mais des difficultés s'y attachent aussi, notamment : l'établissement de normes très différentes, la dispersion des compétences et le risque que certains domaines peu considérables mais importants demeurent complètement négligés.

Selon une autre conception, sensiblement plus académique, on chercherait à élaborer une échelle des informations en commençant par les plus délicates, telles les habitudes sexuelles, et en terminant par les moins délicates, par exemple celles qui sont déjà accessibles au public, dont l'adresse et le numéro de téléphone. L'Université d'Oslo, à l'occasion d'une étude pour le compte du

ministère danois de la Justice, a élaboré une méthode de ce type. Mais une difficulté insurmontable caractérise ces méthodes : tout élément d'information ne devient délicat et important qu'en fonction des circonstances de l'utilisation. Si toutefois il n'est pas possible d'établir une échelle objective du caractère délicat des informations, les données de toute banque d'information particulière peuvent être classées d'après le principe voulant que les règles varient selon les classes, comme dans l'exemple où les dossiers de la police comportaient la distinction entre casier judiciaire et données d'investigation.

Il importe encore davantage de distinguer nettement la réglementation des banques d'information en matière de vie privée et la réglementation des banques elles-mêmes. Le contrôle des banques d'information du point de vue de la vie privée ne doit pas s'étendre à l'information même. Le cas échéant, les résultats, dont la censure et le tri des données, pourraient être bien pires que le mal auquel la réglementation tendrait à remédier. En conséquence, le Groupe d'étude érige en principe que si un type de réglementation était adopté, il faudrait le limiter aux activités des banques d'information touchant la vie privée.

4. Les mécanismes de réglementation

La plupart des projets de réglementation visent les pratiques des banques d'information ; ils comportent une législation et un mécanisme administratif qui, bien que variable selon les propositions, participerait à la mise en œuvre des règlements. Cependant ce rôle pourrait aussi reposer entièrement sur les tribunaux ordinaires ou sur un mécanisme administratif, mais les tribunaux auraient à trancher, en dernier ressort, les questions de droit que soulèverait le fonctionnement des banques d'information. Les mécanismes peuvent revêtir trois formes : tribunal de réglementation indépendant, organisme de surveillance et organisme des griefs ou de protection du citoyen. Nous les étudierons plus bas. Ils ne s'excluent pas entre eux : l'adoption d'un projet de réglementation comportant des éléments des trois est fort concevable.

Les lois générales sur les banques d'information ou celles régissant des activités particulières comportant le recours aux banques d'information (notamment dans le domaine bancaire) pourraient comprendre des règles ou principes d'exploitation. Si les

mécanismes de réglementation esquissés plus loin supposent des lois d'ordre général, l'autre solution est traitée aussi.

a. Tribunal administratif indépendant

Dans un certain nombre de propositions, on envisage la création d'un tribunal administratif ou office de réglementation qui aurait pour fonction de surveiller les pratiques des banques d'information en ce qui concerne la vie privée et les valeurs connexes. Ce tribunal, s'inspirant des principes généraux établis par un corps législatif, aurait autorité dans les domaines suivants : normes de sécurité, méthodes de collecte des données, exactitude et pertinence de celles-ci, échange de données entre banques, accès aux données par ceux qu'elles concernent et notification. Normalement, le corps législatif définirait les objectifs de l'organisme de réglementation (comme dans le cas du Conseil de la radiotélévision canadienne) et fixerait les principes directeurs, mais s'en remettrait à l'organisme de prendre les décisions dans les cas particuliers et d'élaborer des règlements supplémentaires fondés sur l'expérience. L'organisme de réglementation pourrait surveiller les activités des banques d'information et entendre les griefs. La législation habilitante définirait les catégories d'établissements auxquels elle s'appliquerait, et ceux-ci seraient tenus à la licence. Le ministère suédois de la Justice, dans un rapport récent[3], proposait un régime où il serait interdit de traiter par ordinateur des données de caractère personnel sans avoir obtenu une licence d'un office d'inspection. Et cette licence serait accordée s'il n'y avait pas raison de prévoir d'immixtion indue dans la vie privée. Pour lutter contre pareilles violations, l'office établirait à quelles conditions les données pourraient être recueillies, traitées et communiquées.

Le grand avantage d'un organisme de réglementation officiel tient à ce que celui-ci peut prévenir ou réduire au minimum les occasions d'atteinte à la vie privée par une surveillance constante plutôt que par des sanctions ultérieures. Habilité à délivrer et à révoquer des licences, ainsi qu'à élaborer et à modifier des règlements, l'office, appuyé sans doute de conseillers compétents, pourrait assurer toute la souplesse nécessaire pour répondre aux exigences naissant d'une technologie en évolution rapide.

Les faiblesses de cette conception viennent de ce qu'un organisme officiel de réglementation, même dans les circonstances les plus favorables, est un instrument trop peu maniable pour un domaine aussi délicat que celui de la vie privée. Déterminer si la vie privée a été violée dans tel cas particulier est un acte beaucoup

plus subjectif que celui consistant à établir si telle station de télévision a respecté son quotient de contenu canadien. Élaborer en droit le concept de « sphère d'intimité » marquerait un pas en avant. Toutefois, un champ notable de discrétion se maintiendrait en même temps que la possibilité de décisions arbitraires dans un domaine aussi délicat et complexe.

b. Organisme de surveillance

Dans tout le rapport, nous avons employé des expressions restrictives telles que « atteintes virtuelles » et « circonstances pouvant aboutir à l'immixtion ». Compte tenu de la circonspection caractéristique des auteurs de rapports gouvernementaux, il n'en reste pas moins vrai que, s'il y a inquiétude manifeste chez la population et preuve que des violations sont possibles, il n'a pas été établi dans notre étude ou dans d'autres études sur la question que des atteintes se produisaient couramment. D'autre part, il y a lieu d'être vigilant; nous avons noté aussi le progrès constant, et inexorable semble-t-il, de la technologie.

La commission Younger, au terme de deux années d'étude, a formulé le vœu ci-après : « Que l'État se dote par une loi d'un mécanisme lui permettant d'observer la croissance et les techniques de la collecte de l'information personnelle et de son traitement à l'aide d'ordinateurs ». Aux États-Unis, la *President's Commission on Federal Statistics* a fait une proposition analogue.

Cet organisme pourrait, entre autres fonctions, surveiller les méthodes employées dans la collecte, le stockage et la communication des données, en ayant tout particulièrement égard aux innovations technologiques; il pourrait être habilité à examiner, relativement à la vie privée et aux valeurs connexes, les nouveaux systèmes importants en projet, qu'ils soient du secteur privé – tel le « système bancaire électronique » – ou du secteur public – tel le « système du numéro d'identification unique »; l'organisme pourrait rédiger des rapports et y insérer ses recommandations au gouvernement sur ces nouveaux systèmes; enfin il pourrait être habilité à publier des rapports périodiques sur les pratiques de l'information en matière de vie privée et y faire ses recommandations.

L'organisme n'aurait pas de pouvoirs d'exécution et tiendrait son autorité du crédit que lui vaudraient ses rapports et ses recommandations. S'il remplissait aussi une fonction de protecteur du citoyen, il pourrait recevoir les plaintes des particuliers, les examiner et, au besoin, consigner ses conclusions dans des rapports.

Pour que l'action de l'organisme soit efficace, toutes les banques d'information relevant de lui pourraient être tenues de s'y enregistrer, de lui fournir à cette occasion des renseignements détaillés (qui pourraient être rendus publics) sur la nature de leurs systèmes et sur leur politique quant à la manipulation des données.

L'organisme pourrait jouer un rôle précieux de « détection ». Il constituerait un mécanisme de surveillance publique des nouveaux systèmes d'information importants et pourrait sensibiliser l'État et la population aux dangers présents et éventuels. De plus, ces avantages seraient atteints sans l'immixtion que comporterait nécessairement tout office de réglementation.

L'inconvénient majeur d'un organisme de surveillance résiderait dans l'absence de pouvoirs exécutifs. Il pourrait, par exemple, signaler des insuffisances dans les normes de sécurité, mais ne disposerait pas des moyens d'y remédier. L'organisme apporterait le savoir-faire dont a besoin le Gouvernement pour vérifier dans quelle mesure sont respectées les lois constitutives de ses ministères et autres organismes déjà réglementés quant à la manipulation des données.

c. Enquêtes et examen des griefs

La notion d'*ombudsman* est connue de la plupart des Canadiens. L'institution a été adoptée par six provinces, dont le Québec où le titulaire de la fonction est appelé *protecteur du citoyen.* Le rôle consiste à recevoir les plaintes des particuliers sur la façon dont les organismes gouvernementaux les ont traités et à résoudre, si possible, la difficulté grâce à la connaissance de l'administration publique et à des contacts avec elle. Le protecteur du citoyen n'a pas le pouvoir, en général, de commander au ministère en cause telle ligne de conduite, mais l'efficacité de son intervention tient à son prestige et à ce qu'il est habilité à présenter des rapports, après investigations, à l'assemblée législative.

Dans l'État de Hesse, en Allemagne occidentale, on a nommé un protecteur du citoyen le qualifiant de *commissaire aux données*; il a pour mission de surveiller les opérations des banques d'information qui touchent les personnes. Tout sujet estimant que les pratiques d'un système portent atteinte à son sens de la vie privée peut porter plainte. Le commissaire examine l'allégation et, s'il la trouve fondée, en discute avec la banque d'information. On compte bien que la médiation et des compromis apportent satisfaction au plaignant. Normalement, la banque d'information tend à régler les difficultés à l'amiable dans la plupart des cas, espérant s'épargner

des conséquences fâcheuses : poursuites judiciaires, mention dans les rapports publics du commissaire, voire des mesures législatives proscrivant les pratiques fautives.

Ce régime comporte bien des avantages. Sa structure est simple et suppose beaucoup moins de dépenses publiques que les autres modèles. La fonction pourrait être liée aux préoccupations de liberté civile, notamment au projet de création d'un commissaire aux droits de l'homme. Bien sûr, la confiance qu'inspire le titulaire de la fonction intervient dans une large mesure; cependant, ses conclusions et ses recommandations feront autorité en règle générale et bénéficieront d'une attention immédiate. De plus, le modèle semble répondre précisément aux difficultés que connaissent les citoyens; sous ce rapport, au moins, il offre la solution la plus immédiate.

Pourtant, ce modèle n'est pas sans lacune. Tout d'abord, il ne peut embrasser la situation dans son ensemble, le protecteur du citoyen ne détenant pas les pouvoirs nécessaires pour faire des investigations sur chacune des banques d'information sans une plainte préalable d'une personne qui s'estime lésée. Deuxième lacune, le protecteur du citoyen, en règle générale, ne posséderait pas le savoir-faire technique que suppose, par exemple, l'examen des normes de sécurité. Toutefois, l'existence du mécanisme pourrait bien inciter les banques d'information à s'intéresser davantage aux questions de vie privée.

d. Autres modes de réglementation

La plupart des propositions débouchent sur des règles et des structures. Mais les unes et les autres sont séparables. La réglementation des banques d'information peut être mise en œuvre sans une autorité centrale. Aux États-Unis, le *Fair Credit Reporting Act (1971)*, par exemple, prescrit aux agences de renseignements commerciaux d'accorder aux individus l'accès aux dossiers les concernant et d'aviser toute personne de la création de dossiers sur elle, mais de s'en remettre aux tribunaux des décisions. La législation existante permettrait aux gouvernements d'appliquer les règlements examinés plus haut aux établissements qui tiendraient des systèmes d'information personnelle et qui seraient déjà assujettis à une réglementation de l'État relativement à une partie ou à l'ensemble de leurs opérations. De plus, le régime des banques d'information pourrait être étendu à d'autres établissements par des mesures législatives.

Parmi les lois existantes qui pourraient être utiles à cet égard,

mentionnons celles qui régissent les établissements privés ou d'intérêt public et les ordonnances administratives visant les organismes publics eux-mêmes. Les banques privilégiées, les sociétés d'assurance et certaines sociétés exploitantes de télécommunications seraient de la première catégorie, en ce qui concerne l'État fédéral. En modifiant lois ou réglementations, on imposerait le droit d'accès aux informations personnelles, l'obligation de l'exactitude et des règles visant la sécurité et la communication des données ; ce serait un moyen de réglementer les banques d'information.

Les gouvernements pourraient aussi recourir aux ordonnances administratives pour imposer les règlements des banques d'information aux organismes publics qui manipulent des données personnelles. Les dispositions de la Loi de l'impôt sur le revenu et de la Loi sur la statistique touchant le caractère confidentiel pourraient être incorporées à diverses autres lois, dont celles relatives à l'assistance sociale. De plus, les dossiers administratifs internes, notamment ceux concernant le personnel, pourraient être couverts, aux termes de quelques-unes ou de la totalité des règles traitées plus haut, grâce à une modification des lois régissant les droits et les tâches des fonctionnaires provinciaux et fédéraux. Dans les négociations collectives avec les patrons, divers syndicats ont pris des initiatives en ce domaine.

De plus, la législation relative aux droits et aux fonctions des établissements d'intérêt public tels que les hôpitaux, les commissions scolaires et les universités pourraient, après modification, comprendre des prescriptions touchant les données personnelles. L'Ontario s'est déjà engagé dans cette voie relativement aux dossiers des élèves.

Le principal avantage de cette méthode est d'être applicable à des domaines névralgiques. Sa principale faiblesse tiendrait au manque de structures assurant les « voies légales », l'audition impartiale, le recours, etc. De plus, la protection de la vie privée en droit administratif risquerait d'être aléatoire et inégale.

e. Autoréglementation

Grosso modo, il existe deux types d'autoréglementation. Tel groupe décidera librement de réglementer la conduite de ses membres sous certains aspects. Les exemples vont du code de déontologie élaboré par la *Canadian Association of Credit Bureaus* à la décision par les fabricants de voiture d'accroître la sécurité de leurs produits, exemple où l'imminence d'une intervention de

l'État a servi d'aiguillon. Le deuxième type est celui des professions, tels le droit et la médecine ; l'État prescrit par des lois que pour y accéder il faut être titulaire d'une licence, d'un certificat ou adhérer à une association, puis délègue à celle-ci certains pouvoirs de réglementation et d'exécution à l'égard des membres.

L'autoréglementation, d'un type ou de l'autre, impose manifestement un fardeau à ceux auxquels elle s'applique : ceux-ci doivent subordonner leur intérêt à celui de la population là où elle ne dispose pas de moyens directs de l'exprimer. Lorsque l'autoréglementation est entièrement libre, les membres du groupe – par exemple l'*Association of Credit Bureaus* – n'ont pas d'autres pourvoirs que la persuasion morale pour obtenir la discipline ; tout membre peut continuer à exercer la profession même s'il est expulsé. L'autoréglementation libre a sans doute ses avantages ; elle peut créer, par exemple, une obligation morale sans qu'il soit nécessaire d'établir des structures administratives ; mais elle serait trop limitée, semble-t-il, pour constituer à elle seule la principale protection de la vie privée.

Il convient peut-être d'accorder plus d'attention à l'autoréglementation sanctionnée par l'État pour les préposés aux ordinateurs (le personnel informatique) ou aux entreprises (banques d'information, services de travaux à façon). L'autoréglementation appuyée de pouvoirs exécutifs serait de nature à assurer des normes élevées et à protéger le public contre l'incompétence. D'autre part, l'autoréglementation sanctionnée par l'État comporte souvent le risque d'être exploitée comme moyen de promouvoir les intérêts de la profession et de restreindre la concurrence. Le directeur d'une association professionnelle risque d'être partagé entre les intérêts de ceux qu'il représente et les intérêts de la population.

On fera valoir que le droit et la médecine, par exemple, ont besoin d'être bien vus du public pour attirer la clientèle et qu'il en est résulté, jusqu'à un certain point, une conformité entre les intérêts de ces professions et ceux du public. Même si tel est le cas, ce qui est loin d'être établi, il semblerait plutôt que dans le secteur informatique les intérêts de la profession divergent de ceux du public. Les clients des services informatiques ne sont pas les personnes rejointes par la collecte des données, mais des sociétés et des établissements considérables. La mise en œuvre de mesures lentes et chères pour protéger le caractère privé des données sur les personne ne serait pas aussi manifestement avantageuse pour les entreprises informatiques que pour les professions.

De plus, nombre de faits qui ont généralement abouti à l'autoréglementation dans d'autres professions ne semblent pas

intervenir en informatique, notamment le fait que les effectifs viennent de milieux et de disciplines d'une grande diversité. La *British Computer Society* a quand même pris une initiative que beaucoup d'autres associations nationales semblent vouloir imiter : elle a donné un statut professionnel aux informaticiens et élaboré un code de déontologie à leur intention.

Il est nombre de domaines où l'État n'intervient ni ne doit intervenir. Dans une étude effectuée pour nous, on cite le juge Douglas de la Cour suprême des États-Unis :

> Généralement parlant, l'État ne peut agir efficacement que par prescriptions. Aussi de grandes sphères du comportement et de l'activité restent-elles intouchées ; une partie est susceptible d'une réglementation d'État, mais elle est trop petite pour un contrôle satisfaisant ; une autre partie échappe au domaine du droit et déborde sur celui de l'éthique et de la moralité. Ces grandes sphères ne peuvent être rejointes, et d'une façon efficace, que par l'autoréglementation (self-government).

Un exemple d'autoréglementation efficace nous est fourni par le *York University Behavioural Research Institute* qui a établi un code d'éthique pour toute la recherche effectuée sous ses auspices. Un certain nombre d'autres universités ont créé des commissions d'éthique ou envisagent de le faire. L'autoréglementation peut sensibiliser les membres d'un groupe ou un secteur économique à des responsabilités sociales qui, autrement, auraient été méconnues ou négligées. Elle peut leur apporter une plus grande confiance du public. Elle peut réduire le besoin d'une intervention de l'État, considérations importantes pour certains utilisateurs de données sur les personnes, notamment en recherche sociologique.

Pour toutes ces raisons, il faut sûrement encourager toute mesure favorable à l'autoréglementation en ce qui concerne la vie privée des personnes faisant l'objet de fiches. D'autre part, il ressort des autres témoignages que ces mesures ne sauraient à elles seules résoudre tous les problèmes.

5. Réglementation des activités gouvernementales

Parmi les mémoires présentés au Groupe d'étude et ceux auxquels il avait accès, il s'en trouvait deux émanant de ministères fédéraux et deux autres émanant d'organismes provinciaux où l'on signalait les obligations incombant aux gouvernements du fait de

leur prédominance dans la collecte, le stockage et la diffusion des données au Canada. L'O.C.D.E., qui a effectué plusieurs études en ce domaine, concluait en ces termes :

> « Ce sont les gouvernements qui peuvent faire le plus [à cet égard] car ils sont les plus assidus dans la collecte, l'analyse et la communication des informations ; ils sont donc les mieux placés pour mettre en œuvre des normes élevées et donner le bon exemple. »

Si les organismes gouvernementaux recueillent et stockent des quantités massives de données, c'est entre autres, que des prescriptions légales supposent la collecte d'informations détaillées sur les personnes. Le mouvement des données entre individus et établissements dans le secteur privé ne s'accompagne pas de pareilles fonctions. L'application des lois et la sécurité de l'État donnent lieu également à des accumulations massives de données. Ajoutons qu'une grande quantité d'information personnelle recueillie par les gouvernements a trait aux prestations sociales : pensions, allocations familiales, etc. Ces mesures et les masses de données qu'elles nécessitent font intervenir un grand nombre de ministères, ainsi que d'organismes fédéraux, provinciaux et municipaux ; cette dispersion entraîne souvent des doubles emplois et une prolifération superflue des dossiers sur les personnes.

Certains voient dans cet éparpillement une garantie non négligeable de la vie privée. Rappelons que le débat sur l'ordinateur et la vie privée a été lancé aux États-Unis en 1965 au milieu de la fureur engendrée par la vaine proposition d'une banque d'information centralisée et complète, à l'échelon national.

Comme la décentralisation de l'information demeurait la règle dans l'administration publique, les projets de réglementation des banques d'information gouvernementales orientés vers la sauvegarde de la vie privée mettent l'accent sur la communication et le partage des données entre les différents organismes, lesquels se pratiquent souvent d'une façon à la fois arbitraire et voilée du public. L'objectif, *grosso modo*, est de soumettre à des règles la manipulation gouvernementale des données et de la rendre apparente.

Bien sûr, la réglementation des banques d'information gouvernementales n'implique pas nécessairement l'autoréglementation. Cette dernière a été proposée également et elle pourrait être mise en œuvre par des instructions administratives internes qui, bien que n'ayant pas l'effet d'une loi, obligeraient plus que l'autoréglementation du secteur ou de la profession ; c'est que ces instructions bénéficieraient d'un caractère semi-public et du crédit de l'État.

Toutefois, ces propositions visant les banques d'information gouvernementales comportent des règlements ayant les effets d'une loi; leur application relèverait d'un organe gouvernemental distinct; quant à leur exécution, elle incomberait à cet organe ou aux tribunaux. Les propositions enbrasseraient bon nombre des formes propres à la réglementation générale. En Grande-Bretagne, le projet sur le contrôle de l'information avait pour objet de réglementer toutes les banques d'information, y compris celles de l'État.

Néanmoins, certains faits propres au gouvernement tendent à limiter les possibilités en matière de structures applicables aux systèmes gouvernementaux. De plus, d'autres mécanismes de réglementation s'offrent au gouvernement, même s'ils sont inutiles dans le secteur privé.

La formule d'un tribunal administratif indépendant qui attribuerait les licences serait particulièrement inadaptée aux systèmes gouvernementaux. Ce tribunal a été conçu pour réglementer les entreprises en concurrence à la lumière des politiques économique et sociale du Canada. On sauvegarde son indépendance à l'égard du gouvernement afin qu'il puisse se prononcer hors des influences de tout parti politique sur les droits et les plaintes de l'individu.

La réglementation des banques d'information, au gouvernement, est toute différente. Elle ne s'applique pas aux activités commerciales ni aux plaintes individuelles. L'intérêt d'une banque d'information gouvernementale n'est pas d'ordre économique; l'inviolabilité de la vie privée ne l'est pas non plus pour l'individu. Si l'un et l'autre s'opposent parfois, ce n'est pas au sens commercial. On a d'autant moins besoin d'une réglementation pour assurer l'indépendance à l'égard du Gouvernement.

Par ailleurs, il semblerait probablement inacceptable qu'un organe du gouvernement soit autorisé, en particulier par un organisme indépendant, à remplir une fonction de caractère nettement exécutif.

Pour la réglementation des banques d'information de l'État, il existe bien d'autres formes possibles. Aux États-Unis, la *President's Commission on Federal Statistics* a proposé la création, à titre provisoire, d'un organisme uniquement consultatif. Cet organisme collaborerait avec les services de l'État aux tâches ci-après : perfectionner la protection de la vie privée et les garanties connexes, enquêter sur les pratiques portant atteinte à la vie privée, entendre les plaintes et proposer les changements qui pourraient s'imposer. Sa principale utilité serait de rendre le public plus

conscient des systèmes, et de leur action sur la vie des individus et de lui faire mieux connaître les établissements et leur personnel. Sa principale sanction serait l'opinion publique. Toutefois, son efficacité serait compromise par l'absence d'un mécanisme d'exécution. Il lui serait cependant loisible de remédier à cette lacune en faisant passer ses recommandations par une autorité habilitée à intervenir.

On a envisagé d'établir la fonction de réglementation au sein d'un service existant plutôt que de créer un organisme nouveau. Mais il y aurait là un écueil si le service en question maintient déjà ses informations sur les personnes pour soutenir ses propres activités. Un conflit d'intérêt pourrait découler d'une situation qui permettrait peut-être à l'organisme de réglementation de se transformer en une super-banque d'information.

Dans l'administration publique, le pouvoir de contrôle sur les dépenses occupe une place prééminente. La fonction de réglementation pourrait donc se modeler sur les services qui détiennent ce pouvoir dans les ministères. Si, par exemple, il incombait à ces services de définir les normes concernant le caractère privé et confidentiel et d'en surveiller l'application en ce qui a trait aux banques d'information des divers ministères et aux pratiques s'y rattachant, ou de sanctionner les dépenses après qu'un organisme distinct aurait agréé ces banques, les services centraux pourraient faire respecter ces normes grâce au contrôle financier qu'ils exercent. Ce modèle présente toutefois un inconvénient majeur : celui de ne pas être apparent. Les particuliers ne seraient pas en mesure de suivre le processus de réglementation ; ils ne disposeraient donc d'aucun mécanisme pour faire entendre leurs plaintes et n'auraient peut-être même pas connaissance des utilisations des données sur leur compte. Pour remédier à ce défaut, il faudrait attribuer un pouvoir de décision aux tribunaux en la matière ou charger un protecteur du citoyen d'examiner les plaintes.

6. Considérations constitutionnelles

Les divers projets de réglementation ont été examinés au mérite dans le présent chapitre ; ainsi était mise de côté la question, importante pour le Canada, de la répartition des compétences pour réglementer les banques d'information. Faute de propositions d'ordre législatif définies, on ne saurait se prononcer avec précision sur le partage des pouvoirs entre le Parlement fédéral et les corps législatifs provinciaux. Une orientation préliminaire est quand même possible.

Les provinces possèdent manifestement des pouvoirs étendus pour réglementer les systèmes d'information automatisés, puisque sont de leur ressort la propriété, les droits civils, les travaux et les ouvrages d'une nature locale et, d'une façon générale, toutes les matières purement locales ou privées. Par contre, aucune province ne peut légiférer dans les domaines attribués au Parlement. Si les banques privilégiées sont assujetties à de nombreuses lois provinciales, les provinces ne peuvent en réglementer les opérations non plus que leur automatisation. De plus, le pouvoir législatif de la province est limité à son territoire, ce qui exclut les affaires interprovinciales et internationales, qui sont du ressort fédéral.

Le Parlement, lui aussi, a des pouvoirs étendus dans le domaine qui nous intéresse ici. Ceux qui concernent les banques et les sociétés exploitantes de télécommunications comptent sans doute parmi les plus importants. Le Parlement, qui possède le pouvoir de légiférer en matière pénale, pourrait imposer certaines règles de conduite aux exploitants de banques d'information, entre autres. Il a une compétence très étendue pour réglementer les activités qui débordent les frontières provinciales. C'est que lui ont été attribués le commerce, les ouvrages et travaux s'étendant à plus d'une province ou servant de liaison entre deux ou davantage, ou encore qu'une activité ou une matière est d'une importance nationale telle que s'y applique la disposition de l'A.A.N.B. concernant la paix, l'ordre public et la bonne administration. À quel point ou stade une activité cesse-t-elle d'être purement provinciale et se rattache-t-elle à des activités extérieures pour passer dans le domaine de la compétence fédérale ? Voilà une question juridique très complexe, et qui suppose un examen attentif de l'activité en cause, de l'état de l'industrie ainsi que de la nature et de la forme du « remède » recherché. Pour ce qui est de leurs propres opérations, d'autre part, le gouvernement fédéral et les gouvernements provinciaux jouissent de pouvoirs à peu près illimités. Cela tient surtout à ce que les plus grandes quantités de données personnelles sont stockées dans les banques d'information de ces gouvernements.

7. Considérations internationales

Les systèmes d'information canadiens renfermant des données sur les personnes ont beaucoup en commun avec ceux des autres pays occidentaux ; mais ils ont ceci de particulier qu'un nombre important de banques d'information sont établies, en totalité ou en partie, hors des frontières du Canada ; elles échappent donc aux

lois canadiennes, que celles-ci aient trait à la vie privée ou à d'autres questions.

Nos conclusions sur les données canadiennes « extra-territoriales » sont exposées plus haut dans le présent rapport[4]. Certains énoncés généraux ont quand même leur place ici : le volume de ces données est considérable et en croissance selon toutes les indications ; une bonne partie est d'un caractère personnel, car elle se rattache aux points suivants : solvabilité et situation financière, dossier médical, organisation de voyages, etc. ; les données sur les Canadiens sont stockées hors du Canada pour des raisons de rentabilité, sauf exceptions ; à l'heure actuelle, il n'y a pas de réglementation qui tende à réduire ce mouvement de données ou à en tenir état.

Le stockage de données canadiennes outre frontière soulève un certain nombre de questions qui sont extérieures au domaine du Groupe d'étude. Par exemple, il y a perte d'activités économiques, la souveraineté canadienne risque d'être entamée et, enfin, des ressortissants d'autres pays auraient plus facilement accès à des données sur les Canadiens que les Canadiens eux-mêmes. Un problème connexe, soit l'immixtion dans notre vie culturelle, tient aux systèmes d'information exploités par des Canadiens et contenant des données qui proviennent exclusivement ou principalement de sources non canadiennes. Le Groupe d'étude toutefois a limité son attention aux questions de vie privée qui se rattachent à l'information stockée hors des frontières, et en particulier aux États-Unis, pays où est conservée la plus grande partie des données canadiennes se trouvant hors du Canada.

D'après les demandes de renseignements du Groupe d'étude auprès de treize grandes banques d'information américaines détenant d'abondantes données sur les Canadiens, il semblerait que ces données – sauf en un cas et pour des raisons de commodité – ne sont pas distinguées de celles d'une autre origine. La législation américaine, notamment le *Fair Credit Reporting Act*, protège sans doute mieux que la nôtre les personnes faisant l'objet d'informations qui sont stockées et diffusées. Il y aurait en outre une sorte de « débordement » des États-Unis sur le Canada : en effet, les agences canadiennes de renseignements commerciaux, la plupart étant des succursales ou des filiales d'organisations américaines, appliquent la réglementation américaine des compagnies pour des raisons de normalisation même si la législation canadienne ne les y oblige aucunement. Si la législation canadienne n'évolue pas parallèlement à celle des autres pays, le Canada pourrait fort bien devenir un refuge où les banques d'information des États-Unis et

des autres pays étrangers viendraient pour se soustraire à des exigences plus rigoureuses. L'O.C.D.E. a accordé beaucoup d'attention dans ses études à la question du « refuge des informations ».

Le principal problème ne tient donc pas à la violation de la vie privée de Canadiens faisant l'objet de données stockées aux États-Unis[5]. Les difficultés les plus graves sont plutôt les suivantes : une part du traitement des données et des télécommunications est perdue pour les Canadiens du fait de ce mouvement étranger ; les données conservées dans des banques d'information américaines pourraient être bloquées pour toutes sortes de raisons, notamment en vertu de réglementations touchant la sécurité, d'injonctions de tribunaux américains, etc. ; des modifications des lois aux États-Unis pourraient y réduire la protection dont jouissent les Canadiens ; le Canada, en tant que pays souverain, éprouve embarras et contrariété devant les quantités croissantes de données sur les Canadiens, souvent délicates, qui sont stockées en territoire étranger.

Tous ces problèmes ont suscité au moins quatre projets d'une politique gouvernementale qui s'appliquerait notamment au stockage de données sur des Canadiens dans des banques d'information étrangères, et en particulier américaines. Il conviendrait d'accorder à ces propositions un examen plus approfondi que l'analyse préliminaire du Groupe d'étude.

Selon une de ces propositions, il y aurait lieu de s'abstenir de toute intervention et de s'en remettre à la protection de la législation américaine, mais cette voie comporterait de graves inconvénients. La législation américaine pourrait bien subir des modifications et ne plus offrir de garanties suffisantes, hypothèse évoquée plus haut. D'une manière générale, il n'est sûrement pas opportun de nous en remettre à des lois étrangères de l'application de la politique ou des normes canadiennes.

Une autre solution serait de laisser se poursuivre le mouvement actuel par delà la frontière et d'exiger que les sociétés stockant des données dans des banques d'information étrangères s'enregistrent auprès du gouvernement ou d'un organisme à cette fin. Elles seraient tenues, par exemple, de fournir à cette occasion les renseignements ci-après : raison sociale, lieu d'établissement, structure de la banque, principales caractéristiques de fonctionnement, catégories d'informations stockées et fréquence de l'accès à celles-ci. Elles pourraient être tenues en outre d'aviser le service d'enregistrement — et peut-être les personnes faisant l'objet de données — de tous les cas où des informations seraient stockées à l'étranger. Le rapport du Groupe d'étude sur la téléinformatique

propose une structure pour cet organisme. À l'échelon fédéral, l'enregistrement serait obligatoire pour tous les services informatiques et toutes les banques d'information reliés à des réseaux comportant des terminaux en utilisation régulière dans plus d'une province ou se prolongeant en pays étrangers.

Cette méthode établirait pour la première fois une représentation détaillée du mouvement de l'information numérique par delà la frontière. Elle servirait à la fois de guide et de source de connaissances à partir desquelles on pourrait élaborer les mesures nécessaires, notamment des encouragements aux banques d'information à s'établir au Canada et à accroître la proportion du « contenu » canadien dans les systèmes d'information répondant à des besoins économiques et sociaux du Canada. Tout ce programme présenterait toutefois, semble-t-il, l'inconvénient de la lourdeur.

Troisièmement, on pourrait pousser un peu plus loin la méthode ci-dessus et exiger que soit conservé au Canada un double de tous les dossiers. Cette solution serait encore moins souple et fort coûteuse par surcroît. De plus, elle accroîtrait peut-être le risque de violations de la vie privée, puisque les données seraient conservées et manipulées à deux endroits au lieu d'un seul. D'autre part, elle permettrait aux Canadiens de vérifier l'exactitude des informations les concernant, à condition qu'on leur en assure l'accès.

Quatrièmement, on pourrait tenter de prévenir le stockage hors du Canada de données sur les Canadiens. Cette voie extrême serait peu désirable, car elle gênerait l'échange d'informations et par conséquent le commerce international. D'ailleurs, il serait impossible de la mettre en œuvre, étant donné les nombreux moyens de transport et de communication de données. Des variantes de cette option tendant à réduire le mouvement des informations par le biais du fisc et de réglementations de l'accise touchant les données soulèveraient les mêmes objections.

Comme les États-Unis sont les principaux intéressés par rapport au Canada, on a envisagé, au delà de la législation nationale, la recherche d'un accord bilatéral sur le stockage de données par les ressortissants de chacun des deux pays dans le territoire de l'autre. Cet accord pourrait prévoir un engagement de la part de chaque pays à ne pas refuser aux ressortissants de l'autre l'accès aux données les concernant; il porterait création de règles relatives à l'accès aux données par des tiers, par les tribunaux, par les courtiers en informations, etc.; des règles de vérification seraient possibles également.

Cette méthode, tout avantageuse qu'elle soit, soulèverait des difficultés. Le droit de la vie privée n'aurait pas nécessairement

atteint le même développement dans les deux pays ; les lois régissant l'admissibilité des preuves devant les tribunaux ne seraient pas les mêmes ; la situation constitutionnelle du Canada est particulière et elle exigerait une étude complète ; les États-Unis ne consentiraient peut-être pas à isoler la question des données de celle du commerce entre les deux pays.

Dans l'élaboration de politiques internationales en ce domaine, il faudra probablement examiner la question de l'ordinateur et de la vie privée comme étant reliée au mouvement général des marchandises et des services à la frontière.

On a aussi proposé, outre les ententes bilatérales, un examen poussé de ce que pourraient apporter des accords multinationaux sur la vie privée et le mouvement des données entre les pays. Qu'on ne doive ni empêcher ni gêner ce mouvement, cela semble bien établi, tant en ce qui concerne le principe de la libre circulation des informations entre les pays que du point de vue pratique de son utilité.

Il conviendrait probablement d'envisager une convention internationale tendant à sauvegarder la vie privée ; on y déclarerait souhaitable la libre circulation des informations et, peut-être, y insérerait-on des réglementations types concernant la protection des personnes faisant l'objet de données. Ce serait sans doute mettre en valeur l'importance de normes nationales relatives à la vie privée et encourager l'harmonisation des dispositions législatives régissant cette protection sous diverses compétences. Ces réglementations pourraient, comme dans le cas des ententes bilatérales mais dans une perspective plus générale, embrasser les normes de sécurité des données, le droit d'accès pour chacun à son dossier, le droit de vérification, l'accès aux données pour les tiers, etc. Cette convention serait conforme à l'article 12 de la Déclaration universelle des droits de l'homme, qui, rappelons-le, stipule le droit à la vie privée. Le Pacte international des droits civils et politiques (1966), auquel le Canada n'est pas partie, prévoit une protection semblable.

Une convention pourrait faire état des incidences internationales de la question de l'ordinateur et de la vie privée, et faciliter le mouvement international des informations. Elle pourrait aussi faire opposition aux points de vue de ceux qui voudraient restreindre le mouvement des informations et qui avancent que les Canadiens seraient probablement moins bien protégés si les données sur eux étaient stockées à l'étranger.

Un grand nombre de pays effectuent ou se proposent d'effectuer des études sur l'ordinateur et la vie privée. La France, lors

d'une réunion récente de l'O.C.D.E., a fait valoir combien il importe que les diverses législations nationales sur la vie privée soient compatibles. L'Association internationale des avocats mène actuellement, pour le Conseil européen des ministres, une étude qui comportera, notamment, l'élaboration d'articles touchant la protection de la vie privée et des activités non publiques des entreprises. L'Union internationale des télécommunications doit examiner la question de la vie privée sous l'angle des liens entre télécommunication et banques d'information.

Le Groupe d'étude n'a pas encore examiné les questions constitutionnelles que peut soulever la mise en œuvre d'accords internationaux. Quoi qu'il en soit, la collaboration fédérale-provinciale sera sûrement indispensable.

Enfin, comme le Canada, sur le plan international, tend surtout à assurer des droits dont les Canadiens jouissent dans leur pays, encore faut-il qu'ils soient d'abord établis clairement dans la législation canadienne.

[1] Études effectuées pour notre Groupe par C. Fabien, K. Katz, J. Sharp et S. Usprich.

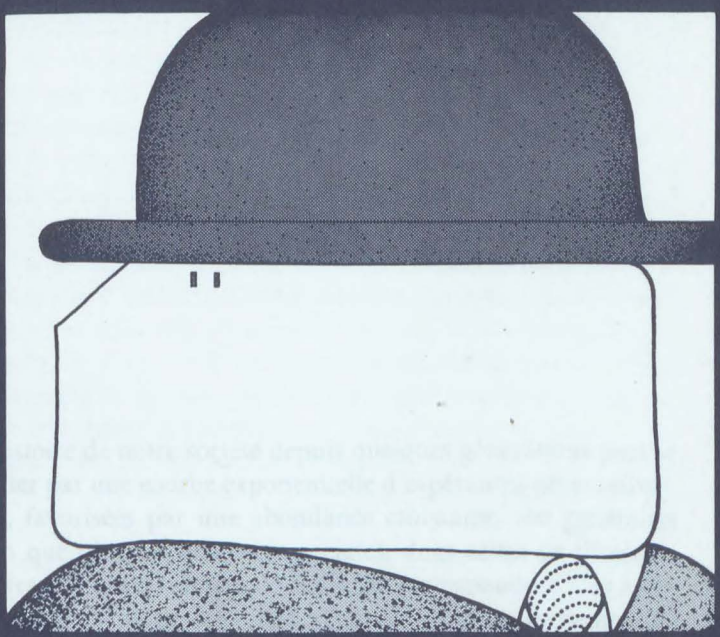
[2] Le rapport de l'Académie nationale des sciences (États-Unis) portera sur des questions analogues. Il doit paraître cet automne.

[3] Une distinction subtile de la *President's Commission on Federal Statistics* s'appliquerait à l'utilisation par les corps policiers des informations recueillies par les gouvernements aux fins de l'assistance sociale. La Commission propose qu'on ne communique des données que pour la réglementation du régime. Ainsi un service social ne serait pas tenu de transmettre à la police des informations propres à établir un rapport entre le sujet demandant de l'assistance et la délinquance, mais fournirait des renseignements établissant que le sujet a fraudé l'assistance sociale.

[4] « Les ordinateurs et la vie privée », résumé du rapport (S.O.V. t972:47) et Proposition de loi sur l'information confidentielle présentée par la Commission d'enquête sur la publicité et le caractère confidentiel des documents de l'Administration.

[5] Après que le Groupe d'étude eut terminé ses enquêtes et ses recherches, la presse accorda beaucoup d'attention à une pratique nouvelle, adoptée dans les grands magasins et les supermarchés des provinces de l'Ouest, selon laquelle les clients s'identifient par l'empreinte du pouce pour les paiements par chèque; ces empreintes sont controlées dans une banque d'information automatisée à Fort Worth, au Texas.

Sixième partie



Pour conclure

Chapitre 13
Postface

L'histoire de notre société depuis quelques générations peut se représenter par une courbe exponentielle d'espérances progressives. Celles-ci, favorisées par une abondance croissante, ont généralisé l'opinion que diverses exigences sociales, dont celles de l'instruction, du travail et des services de santé, ne correspondent plus à des privilèges mais à des besoins fondamentaux de la vie contemporaine. À ces trois exigences s'ajoute aujourd'hui celle de l'intégrité du milieu. Enfin, le « droit à la connaissance » et le « droit à la vie privée » font désormais l'objet des espérances d'ordre moral.

Quelle que soit la probabilité qu'on trouve dans le droit naturel, le droit écrit ou une théorie politique, un fondement au « droit à la vie privée », à supposer que ce soit utile, l'important est de noter qu'on souhaite de plus en plus, sauf erreur, que ce droit soit reconnu socialement et juridiquement. Il s'ensuivrait, du point de vue de l'information personnelle, qu'il est légitime pour l'individu de ne pas permettre que des informations le concernant soient communiquées à des tiers à son insu ou sans son consentement, sauf si des valeurs sociales opposées ont préséance sur ses intérêts, et sous réserve, en ces circonstances, de dispositions de la loi.

Le « droit à la connaissance » est la « liberté de l'information », en termes plus courants, c'est-à-dire un objectif qui parfois se concilie mal avec celui de la vie privée. Ce conflit ne peut guère se résoudre par des formules abstraites ; il convient plutôt de l'aborder relativement à des situations concrètes, bien qu'il demeure nécessaire d'élaborer une politique générale de « liberté d'information ». Dans le présent rapport, nous montrons qu'il importe de bien distinguer réglementation protégeant le caractère privé de l'information et réglementation de l'information : cette dernière entraverait le mouvement de l'information.

L'enquête du Groupe d'étude a aussi mis en relief une inégalité de pouvoir entre particuliers et organisations découlant en partie d'une inégalité dans l'accès à l'information. Le débat sur la vie privée embrasse manifestement des questions politiques et des questions purement juridiques. La crainte de ne plus pouvoir jouir de la vie privée intervient moins dans les premières que celle de voir les organisations accroître leurs aptitudes à manipuler les individus et à les soumettre grâce à la possession de systèmes d'information considérables et efficaces. Il est impossible de ne pas tenir compte de ces craintes, mais on ne saurait non plus les apaiser par de simples mesures de protection de la vie privée. Les solutions résident dans un meilleur partage du pouvoir que confèrent les systèmes d'information automatisés. L'information est un sujet délicat, tout comme la vie privée et l'informatique, d'ailleurs. Il ne faudrait pas délimiter trop rigidement les débats bien informés et les réactions aux problèmes qui se posent.

Des préjudices peuvent être portés aux individus par le simple volume de la collecte des données, qui risque de devenir presque une fin en soi et, en certains cas, un moyen de créer du travail. Il faudra un jour fixer des limites – si possible, avant que tout soit connu sur chacun et sur toute chose. Une analyse de rentabilité ou le recours au bon sens hâteraient sans doute ce dénouement. À brève échéance, il semble bien que dans l'administration publique, l'entreprise et les universités, les responsables devront envisager sérieusement l'opportunité de critères ; ceux-ci, fondés peut-être sur les notions d'utilité, d'efficacité et de sauvegarde de la vie privée, permettraient d'établir ce que peut valoir une collecte sans fin des données.

Les méthodes de collecte varient tout autant que l'éventail des gens qui s'y adonnent, depuis l'agent de police jusqu'au spécialiste des sciences sociales. Les procédés d'investigation des corps de police ont fait l'objet de débats internes et publics ; les arrêts des

tribunaux contribueront à déterminer dans quelle mesure sont recevables les éléments de preuve obtenus par tables d'écoute.

Quand aux spécialistes des sciences sociales, la situation est plus complexe. S'il faut rechercher la connaissance, il est peu de domaines où soit aussi délicate pour nous la critique du libre mouvement de l'information. Nous avons noté toutefois, et loué implicitement, l'élaboration par le *Behavioural Research Institute* (Université York) d'un code d'éthique applicable à ses propres activités. Malheureusement, ces codes sont plutôt rares. Pourtant les organismes de recherche et les universités auraient intérêt à envisager pareille initiative. On peut aussi aborder le problème d'une autre façon, soit celle de la *Russell Sage Foundation* (États-Unis) qui impose un code d'éthique pour toutes recherches s'effectuant sous ses auspices. Il serait souhaitable que le Conseil des Arts, le Conseil national de recherches, le Conseil de recherches médicales du Canada et d'autres organismes d'aide financière examinent s'il y a lieu d'établir un code d'éthique semblable en collaboration avec, par exemple, l'Association des collèges et universités du Canada et le Conseil canadien de recherches en sciences sociales[1]. Ce projet, s'il était adopté, pourrait embrasser tous les travaux de recherche, financés par contrats ou par subventions, qui seraient effectués pour les ministères et organismes. Il conviendra de profiter de l'occasion pour analyser et peser les obstacles à la recherche.

Les méthodes de collecte chez les statisticiens sont également source de préoccupation. Ainsi, le travail pose indirectement le problème de la divulgation par résidu dans le cas des tableaux. À ce propos, un conseiller louait, dans une étude, les normes et les méthodes mises au point par Statistique Canada. Cet organisme est habilité à fixer des normes pour tous les travaux statistiques qu'entreprennent les ministères et organismes, mais ce pouvoir n'a guère été exercé. Peut-être voudra-t-on aussi examiner le vœu formulé dans le rapport récent du *United States Decennial Census Review Committee*, soit qu'on adjoigne au service statistique un comité consultatif qui serait appelé à émettre ses avis sur l'orientation à suivre et sur les questions connexes.

Parmi les voies possibles, l'autoréglementation des banques d'information serait d'une valeur limitée, semble-t-il, mais non négligeable. L'adoption d'un code déontologique par la *British Computer Society* peut s'imposer à l'attention du secteur informatique canadien. Que des mesures analogues aient été adoptées par certaines branches du secteur telles que la publicité et les agences de

renseignements commerciaux, voilà qui démontre les possibilités en ce domaine.

Le recours aux tribunaux a ses limites quand il s'agit de sauvegarder la vie privée face aux systèmes d'information, puisque tant de questions connexes se prêtent mieux aux voies administratives qu'à celles de la justice. D'autre part, l'efficacité des tribunaux s'accroîtra à mesure que le volume des litiges en la matière augmentera et que les tribunaux se sensibiliseront à l'importance de la vie privée. Interviendront en outre l'élaboration et la mise au point d'un recours général. Un concept de vie privée, s'inspirant peut-être de celui de « sphère d'intimité » exposé dans le chapitre 11, serait sans doute utile au gouvernement fédéral et aux gouvernements provinciaux lorsqu'ils établiraient ce droit par législation ou promulgueraient des lois pour régir l'activité d'organisations ou d'industries particulières. Déjà il existe des lois concernant le caractère confidentiel des informations recueillies par Statistique Canada et par le ministère du Revenu national. L'Ontario doit adopter des mesures analogues en ce qui concerne les fiches des élèves.

Les fichiers sur lesquels reposent les décisions sur le crédit des gens et les taux auxquels on leur prête sont les plus importants pour beaucoup de Canadiens. La loi fédérale américaine dite *Fair Credit Reporting Act* est sans équivalent au Canada ; toutefois la plupart des provinces envisagent ou appliquent des mesures réglementant, à divers degrés, les agences de renseignements commerciaux. Ces mesures sont d'une importance manifeste ; il y aurait peut-être lieu d'accorder de l'attention aux entreprises dont l'activité déborde le cadre provincial ou comporte des ramifications internationales.

Il est un autre domaine qui mérite une attention spéciale, soit celui des dossiers médicaux et des fiches de santé. D'ailleurs, il en a été question dans divers mémoires présentés au Groupe d'étude, sans compter que l'*Ontario Medical Association* s'est dotée en 1971 d'une commission de la vie privée. Notons enfin que le ministère américain de la Santé, de l'Éducation et du Bien-être a entrepris récemment une grande étude sur le même sujet.

Les initiatives et les lois dont il est fait état plus haut ne constituent pas de solution d'ensemble, malgré la protection qu'elles assurent. Une réglementation de l'État par l'intermédiaire d'un organisme de surveillance, d'un protecteur du citoyen ou ombudsman ou d'un tribunal indépendant (voir chapitre 12) réuniraient les avantages de l'uniformité et de la souplesse.

Si la question de la compétence constitutionnelle en matière de banques d'information du secteur privé n'a pas été étudiée en

profondeur dans le présent rapport, il serait souhaitable, quand viendra le temps de le réglementer, que les autorités fédérales et provinciales harmonisent leurs points de vue; s'il y a actions séparées à chaque échelon, des consultations étroites seront sûrement utiles. Les Commissaires pour l'uniformité de la législation pourraient assurer la liaison à cette fin.

Le Groupe d'étude est bien conscient que l'État doit d'abord prêcher par l'exemple. Dans la collecte des données, les gouvernements occupent de loin la première place, soit en raison des contrats et des subventions de recherche, soit du fait des programmes administratifs en cours.

On concevrait donc que le gouvernement fédéral, à titre de modèle ou de milieu d'expérimentation, examine s'il serait souhaitable de réglementer les banques d'information exploitées par ses ministères et organismes, pour ce qui est du respect de la vie privée. La protection de celle-ci et des valeurs connexes est, en quelque sorte, un terrain assez peu connu. L'expérience vaudra sans doute mieux que la théorie dans l'élaboration de règles précises et des exceptions à ces règles, qui sont tout aussi importantes. La réglementation sera, au besoin, appliquée avec réserve et, si possible, dans un cadre se prêtant à une certaine expérimentation. Que la protection de la vie privée forme le sujet du présent rapport, voilà qui peut faire oublier les avantages sociaux et économiques qu'offrent les systèmes d'information automatisés; il serait peu sérieux de risquer ces avantages en protégeant la vie privée pour la forme plutôt que dans son essence.

L'instrument servant à réglementer les banques d'information gouvernementales pourrait se présenter sous diverses formes : organisme de réglementation indépendant relevant directement du Parlement; organisme de réglementation relevant d'un ministre et faisant partie de l'Administration; ministère central ayant autorité sur les dépenses dans toute la fonction publique et ayant compétence pour appliquer les règlements administratifs; protecteur du citoyen sur le modèle, ou à peu près, du commissaire aux données dans l'État ouest-allemand de Hesse; la fonction pourrait aussi se rattacher à la commission canadienne des droits de l'homme qui est à l'état de projet. Il importerait d'accorder une attention particulière aux propositions tendant à réunir les avantages du caractère ostensible (protecteur du citoyen) et ceux de l'efficacité quotidienne (règlements administratifs mis en œuvre par un service central).

Si le gouvernement établit que la mise en œuvre de ce type de réglementation est utile, c'est-à-dire s'impose lui-même des

restrictions à l'exploitation de ses propres banques d'information, il aura beaucoup fait pour la sauvegarde de la vie privée.

À diverses reprises, dans le présent rapport, nous avons fait valoir que ni notre étude ni d'autres effectuées à l'étranger n'avaient abouti à la conclusion que les violations de la vie privée sont courantes ou générales. Nous avons aussi noté que les occasions de telles atteintes se produisent effectivement, et exprimé l'opinion que la rapidité du progrès technologique devrait accroître les moyens de léser les intérêts individuels. Au chapitre 12, il est question d'un organisme qui, selon la proposition Younger (Grande-Bretagne), surveillerait la conduite des banques d'information relevant de l'État, étudierait l'évolution technologique, analyserait les projets de systèmes nouveaux, tel celui d'un numéro d'identification unique, et rédigerait des rapports ayant pour objet de renseigner la population et de proposer des orientations à l'État.

Ayant examiné si le stockage à l'étranger de données concernant des Canadiens entraînait des risques particuliers d'atteinte à la vie privée, nous estimons que la localisation des fichiers n'est pas notablement déterminante sous ce rapport. Toutefois, le volume de ces données et leur caractère soulèvent des questions touchant les possibilités d'envahissement culturel plutôt que d'atteinte à la vie privée. Non seulement une activité commerciale sera perdue, mais l'entité fragile qu'est la culture canadienne est sûrement aussi vulnérable, face aux systèmes d'information automatisés qu'aux programmes de radiodiffusion.

L'étendue et la nature de l'information numérique franchissant la frontière posent sûrement des problèmes d'orientation difficiles. Toute tentative pour restreindre ce mouvement d'information soulèverait la grave question d'un contrôle par l'État, que celui-ci soit réalisable ou non. La première mesure à envisager consisterait à obliger par la loi les compagnies et organismes canadiens à s'enregistrer auprès d'un service à cet effet s'ils recouraient largement à des banques d'information établies hors du Canada. Le Groupe d'étude sur la téléinformatique au Canada a justement recommandé la création d'un bureau d'enregistrement des réseaux nationaux d'informatique. Cette mesure permettrait d'établir pour la première fois en quoi consistent les informations numériques qui franchissent la frontière. De plus, le Canada pourrait se doter d'un instrument de surveillance et d'une source de renseignements, et mettre au point les interventions nécessaires. Celles-ci comprendraient peut-être des incitations à établir les banques d'information dans nos frontières et à augmenter la proportion des éléments d'origine canadienne dans les systèmes

d'information pourvoyant à des besoins sociaux et économiques du Canada.

Certains pays européens craignent que les pays qui ne réglementent pas les systèmes d'information quant au respect de la vie privée ou à d'autres valeurs ne deviennent des « refuges » ; la question a même été soulevée dans les délibérations de l'O.C.D.E. Comme il y a accroissement de volume dans les informations franchissant la frontière, le besoin d'une coordination internationale par des moyens législatifs ou autres évolue dans le même sens. C'est à l'Organisation des Nations unies probablement qu'il conviendrait d'étudier ce problème.

En bref, le Groupe d'étude conclut ce qui suit :

- Le terme « vie privée » est trop restreint relativement à toutes les préoccupations que suscitent les systèmes d'information massifs et omniprésents. Il évoque d'une part les griefs politiques touchant le recours aux systèmes d'information par des organismes soucieux d'accroître ainsi leur pouvoir au détriment éventuel des individus, et d'autre part la crainte que les systèmes d'information servent à manipuler les particuliers ou à les soumettre.
- Les principaux points de préoccupation touchant la vie privée et les valeurs connexes qui peuvent être atteintes par les réserves d'information personnelle sont les suivants : quel est le degré d'exactitude des données ? est-ce qu'on a avisé l'intéressé des informations recueillies à son sujet et des usages qu'on pourrait en faire ? à quels contrôles la communication de données à des tiers est-elle soumise ? quelle est la qualité des méthodes de protection ? dans quelle mesure les particuliers ont-ils accès à leurs propres fiches et peuvent-ils en vérifier l'exactitude ?
- La place des ordinateurs n'est pas nettement établie. Ces machines favorisent collecte, stockage et diffusion rapide de quantités croissantes de données. Néanmoins, les informations les plus strictement personnelles sont encore conservées dans des fichiers manuels. Par contre, les ordinateurs se prêtent à une programmation propre à accroître la protection de la vie privée.
- Le Canada connaît des difficultés particulières. Une grande quantité d'informations personnelles sur les

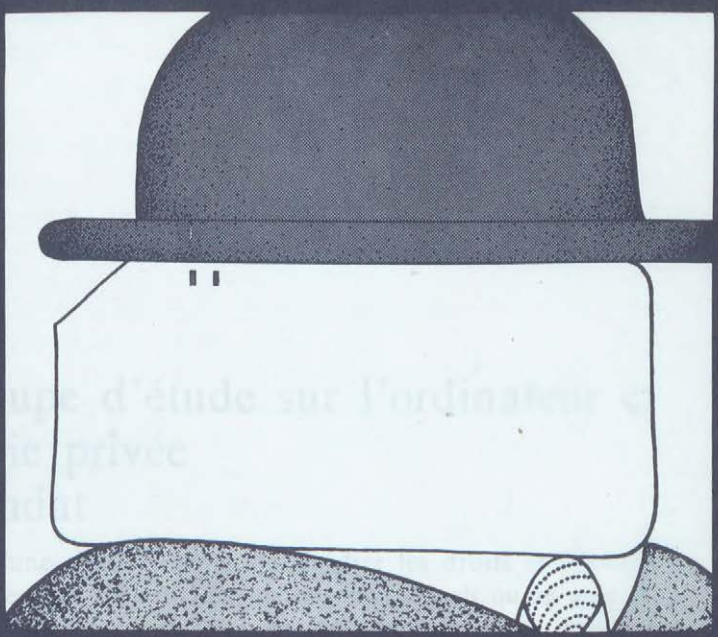
Canadiens, dont une forte proportion de très délicates, sont stockées hors des frontières et par conséquent hors du domaine d'application du droit canadien. Ce mouvement doit être surveillé et noté ; il faut en outre favoriser la formation de banques d'information au Canada.

- Parmi les nombreuses propositions que nous avons examinées, aucune ne semble offrir une solution d'ensemble au problème des atteintes à la vie privée. Mais on observe certaines possibilités particulièrement prometteuses : celle d'un organisme de surveillance et d'un protecteur du citoyen qui entendrait les plaintes des particuliers ; celle de la jurisprudence, si les tribunaux étaient saisis d'un plus grand nombre de réclamations.
- L'État, qui est au premier rang pour le volume des informations qu'il recueille ou fait recueillir, a un rôle clé à jouer. À la solution du protecteur du citoyen et de l'organisme de surveillance, il pourrait ajouter celle de règlements administratifs qui seraient mis en œuvre par un service central ayant si possible la haute main sur les dépenses ; peut-être aussi envisagerait-il l'élaboration d'un code déontologique qui régirait la recherche bénéficiant des fonds publics.

Ayant réfléchi un an à cette question, le Groupe d'étude rejette l'affirmation voulant que les atteintes à la vie privée dans le domaine de l'information soient chose suffisamment courante pour qu'on parle de « crise sociale ». Mais on ne cesse de s'inquiéter. Peu de banques d'information ont été conçues et installées de sorte que le souci de la vie privée constitue un élément de la planification, sauf parfois dans l'intérêt de l'organisation elle-même. La collecte des données et la technologie informatique se développent à un rythme qui ne donne aucun signe de ralentissement. Si, de même, on en vient à attacher une plus grande importance à la sauvegarde de la vie privée, comme certains faits incitent à croire, alors le problème circonscrit que nous avons exposé pourrait bien prendre des proportions tout autres. Contrairement à la crise écologique, qui était prédite mais contre laquelle on n'a rien fait avant que des dégâts graves aient été infligés au milieu, la crise de la vie privée ne se produira pas fatalement. Il est même certain qu'on peut l'éviter par des mesures de prévention appropriées.

1. Le guide des candidats aux subventions de recherche en humanités et en sciences sociales du Conseil des arts (1972) pose la condition suivante :
« Les données que des subventions du Conseil des Arts auront permis de recueillir devront être rendues publiques dans un délai raisonnable, à condition que soient respectés le caractère confidentiel des renseignements et le droit à la vie privée. »

Appendice



Groupe d'étude sur l'ordinateur et la vie privée
Mandat

D'une manière générale, étudier les droits et les valeurs connexes, liés à l'individu, qu'ils soient actuels ou en voie de se constituer, ainsi que les questions découlant des possibilités d'atteintes à la vie privée par la collecte des données que renferment les systèmes d'information et de classement automatisés, de même que par leur stockage, leur traitement et leur exploitation.

a) Déterminer les types d'informations personnelles actuellement stockées, traitées et diffusées, ou qui le seraient dans l'avenir, par le moyen des systèmes d'information automatisés, tant au gouvernement que dans les organisations de toute nature ;

b) examiner les méthodes et les mécanismes de collecte, de stockage, de traitement et de diffusion des informations d'ordre personnel quant à leurs incidences sur le respect du droit à la vie privée et des droits individuels connexes ;

c) apprécier les techniques de protection visant à prévenir l'accès illicite aux systèmes d'information automatisés;

d) étudier les mesures d'ordre juridique, réglementaire, technique ou professionnel susceptibles d'assurer le respect du droit à la vie privée et des droits individuels connexes, et apprécier les facteurs commerciaux, juridiques ou constitutionnels qui pourraient en gêner l'application.

Études effectuées pour le Groupe d'étude

The Nature of Privacy – D. N. Weisstub et C. C. Gotlieb.
Personal Records : Procedures, Practices, and Problems – J. M. Carroll et J. Baudot, Carol Kirsh, J. I. Williams.
Electronic Banking Systems and Their Effects on Privacy – H. S. Gellman.
Technological Review of Computer/Communications[1]
Systems Capacity for Data Security – C. C. Gotlieb et J. N. P. Hume.
Statistical Data Banks and Their Effects on Privacy – H. S. Gellman.
Legal Protection of Privacy – J. S. Williams.
Vie privée et ordinateur dans le droit de la Province de Québec – J. Boucher.
Regulation of Federal Data Banks – K. Katz.
Regulatory Models – J. M. Sharp.
Ordinateur et vie privée : Techniques et contrôle – C. Fabien.
The Theory and Practice of Self-Regulation – S. J. Usprich.
Privacy, Computer Data Banks, Communications and the Constitution – F. J. E. Jordan.
International Factors – C. Dalfen.

Un nombre limité de tirés à part de ces études est disponible. On peut s'en procurer un exemplaire en s'adressant au ministère des Communications, 100 rue Metcalfe à Ottawa, ou au ministère de la Justice, rue Wellington, angle Kent, à Ottawa. Nous en donnons un bref résumé dans les pages qui suivent.

[1] Étude effectuée par le Groupe d'étude sur l'ordinateur et la vie privée en collaboration avec le Groupe d'étude sur la téléinformatique au Canada. Elle sera publiée éventuellement.

Résumés

WEISSTUB, D. N. et GOTLIEB, C. C., The Nature of Privacy.

La notion de vie privée en regard de l'individu – ses craintes et les faits reliés à la concentration des données chez les gouvernements et les organisations et aux modifications dans l'équilibre des forces introduites par l'ordinateur. La menace qui pèse sur les libertés individuelles est analysée d'un point de vue juridique, politique, psychologique, et philosophique à partir d'observations faites au Canada, dans une perspective historique et idéologique.

CARROLL, J. M., Personal Records : Procedures, Practices and Problems.

Enquête sur les systèmes d'information au Canada, particulièrement sur les mesures prises pour préserver le caractère privé des informations. L'auteur étudie surtout les moyens de renforcer les normes de sécurité et d'assurer une meilleure protection à l'information confidentielle dans les systèmes d'information gouvernementaux ou privés. On y examine les méthodes de collecte, de stockage et de communication de ces informations dans treize secteurs d'activité au Canada. Les données à ce sujet proviennent de réponses à un questionnaire, d'entrevues avec des exploitants de banques d'information et des mémoires reçus d'organisations ou d'associations.

GELLMAN, H. S., Electronic Banking Systems and Their Effects on Privacy.

L'auteur décrit quelques banques d'information automatisées et tente de prévoir leur évolution. La question de l'intrusion dans la vie privée par ces banques y est examinée ainsi que les moyens de protéger l'information confidentielle.

Technological Review of Computer/Communications[2]

Il s'agit d'une analyse prospective des développements susceptibles de marquer, au cours de la prochaine décennie, l'évolution de la téléinformatique : matériel, programmerie, télécommunication. Les principales transformations qui pourraient toucher les systèmes de stockage et d'extraction de données personnelles y sont évoquées.

GOTLIEB, C. C. et HUME, J. N. P., Systems Capacity for Data Security.

Études des méthodes qui pourraient assurer la protection des données dans les systèmes d'information automatisés. On y présente une estimation détaillée des coûts de diverses mesures de sécurité et y propose des améliorations possibles aux systèmes et méthodes de protection des données.

GELLMAN, H. S., Statistical Data Banks and Their Effects on Privacy.

Identification des atteintes virtuelles à la vie privée pouvant résulter de la préparation et de l'exploitation des informations statistiques. L'auteur propose des moyens de protection et apprécie leur efficacité.

WILLIAMS, J. S., Legal Protection of Privacy.

Examen des recours qu'offre la *Common law* pour affirmer le droit des individus à la vie privée. L'auteur indique également les limites de cette protection et tente de préciser les intérêts à protéger. Enfin, il met en lumière les domaines où des améliorations peuvent être apportées dans le cadre des lois actuelles.

BOUCHER, J., Vie privée et ordinateur dans le droit de la Province de Québec.

L'auteur examine dans quelle mesure le droit à la vie privée est protégé par la législation du Québec (Code civil et statuts du Québec). Bien que ce droit ne soit pas reconnu comme tel, les lois relatives aux contrats, à la propriété et aux préjudices offrent divers recours. L'auteur recommande que ce droit soit inscrit dans le Code civil comme un droit personnel.

KATZ, K., Regulation of Federal Data Banks.

Étude des différents types de systèmes d'information exploités par le Gouvernement du Canada selon le caractère plus ou moins délicat des informations qu'ils contiennent. L'auteur examine les moyens administratifs ou juridiques à mettre en œuvre pour limiter les intrusions dans la vie privée des personnes, particulièrement les techniques qui seraient applicables aux systèmes d'information du gouvernement fédéral.

SHARP, J. M., Regulatory Models.

Étude des moyens propres à sauvegarder la vie privée des individus qui se trouve menacée par les systèmes d'information, qu'ils soient automatiques ou manuels. On y traite particulièrement des banques d'information au Canada, des règles d'exploitation visant à protéger le caractère privé de l'information personnelle, de l'opportunité pour le secteur informatique de se doter d'un code de déontologie. On y examine tout spécialement certains modèles de réglementation des compagnies de crédit.

FABIEN, C., Ordinateur et vie privée : techniques et contrôle.

L'étude examine et analyse les avantages respectifs des moyens administratifs et des recours judiciaires propres à sauvegarder la vie privée relativement à l'information personnelle. L'auteur y donne un exemple d'autoréglementation et souligne le rôle que peut jouer l'opinion publique sur le plan politique. Peut-être le point saillant de l'étude est-il la proposition de créer un mécanisme administratif de protection du citoyen (ombudsman).

USPRICH, S. J., The Theory and Practice of Self-Regulation.

L'auteur évoque les implications, sur le plan théorique, de l'autoréglementation et tire les conclusions qui s'imposent quant à son efficacité face au danger d'exploitation abusive de l'information personnelle dans le secteur informatique.

JORDAN, F. J. E., Privacy, Computer Data Banks, Communications and the Constitution

Considérations d'ordre constitutionnel sur les systèmes de traitement et d'exploitation des données visant à déterminer, à la lumière des dispositions de l'Acte de l'Amérique du Nord britannique (1867), les compétences respectives des gouvernements fédéral et provinciaux en ce domaine.

DALFEN, C., International Factors.

Étude des problèmes soulevés par l'existence de banques d'information étrangères, essentiellement américaines, détenant des informations sur des Canadiens. L'auteur y examine les problèmes que cela peut susciter pour le Canada, les incidences des lois étrangères touchant les données « extra-territoriales », et les solutions qui pourraient être apportées.

[2] Cette étude sera éventuellement publiée par le Groupe d'étude sur la téléinformatique au Canada.

Questionnaire

Le questionnaire (principale technique utilisée par le Groupe d'étude pour recueillir des informations) a été envoyé à 2 471 compagnies, organismes ou établissements d'intérêt public au Canada. Il avait été éprouvé auparavant auprès de 45 organisations. Le Groupe a reçu 1 268 réponses, dont celles des 24 organisations ayant participé au test préliminaire.

Le texte du questionnaire est reproduit ci-après, ainsi que la ventilation des réponses. L'analyse des réponses a été faite à partir des 1 215 premiers questionnaires reçus. En fait, les résultats n'ont pas été modifiés d'une manière sensible par les réponses qui nous sont parvenues plus tard. (Le symbole ∅ indique le nombre d'enquêtés n'ayant pas répondu à une question donnée.)

Groupe d'étude sur l'ordinateur et la vie privée
Ministère des Communications et ministère de la Justice
Questionnaire

Définitions

Fiche d'un individu : Groupe d'une ou de plusieurs unités consécutives d'information sur un seul individu identifié (par exemple, les antécédents de travail d'un employé, un registre de feuilles de paie).

Dossier : Ensemble de fiches connexes, traité comme une unité, par exemple, un dossier sur tous les employés d'un organisme.

Les *dossiers manuels* sont des fiches (microfilms compris) que l'on entretient et auxquelles on a accès manuellement.

Les dossiers de machines comptables électroniques sont des fiches auxquelles on a accès et que l'on manipule à l'aide de dispositifs électromécaniques, comme des trieuses de cartes, des machines tabulatrices, des interclasseuses, etc.

Les dossiers emmagasinés dans un ordinateur sont des fiches qui sont gardées en mémoire sous forme de carte, de ruban, de disque, de tambour, de tores à ferrites et sont manipulées par un ordinateur.

Section I

Du n° 1 au n° 6, les questions concernent l'organisation et la tenue de vos fiches en général, sans référence à un dossier en particulier ou à l'utilisation d'ordinateurs.

1. A. Numéro d'identification de la personne qui remplira le présent questionnaire.

1. B. Qui va remplir le présent questionnaire ? (Cochez *une* seule réponse).

La personne à laquelle le questionnaire a été envoyé	( )
Une autre personne (précisez)	( )

1. C. Où sont localisés les préposés à l'enregistrement des données ? (Cochez *une* seule réponse).

À l'endroit même où le questionnaire fut envoyé	( )
Autres endroits (précisez)	( )

2. A. Comment caractérisez-vous votre organisme, en ce qui a trait à l'organisation judiciaire ? (Cochez *une* seule réponse). $\emptyset = 55$

Organisme fédéral	(55)
Organisme provincial	(142)
Organisme régional ou municipal	(68)
Association constituée en société fédérale	(283)
Association constituée en société provinciale	(484)
Association constituée en société étrangère	(30)
Autre (précisez)	(98)

2. B. Comment caractérisez-vous votre organisme, en ce qui a trait à ses objectifs ? (Cochez *une* seule réponse). $\emptyset = 26$

Organisme à but lucratif	(588)
Organisme à but non lucratif	(596)

2. C. Comment caractérisez-vous la fonction primordiale de votre organisme ? (Marquez *une* seule catégorie). $\emptyset = 36$

Institution bancaire, de prêt, ou autre institution financière	(57)
Assurance sur la vie ou contre les accidents	(73)

Entreprise de service public	(37)
Publication et radio, communications de masse	(7)
Statistiques de vie et de santé	(179)
Éducation	(73)
Taxation	(1)
Enregistrement des automobiles et délivrance des permis de conduire	(2)
Commerce général	(19)
Cartes et réservations pour les voyages et les spectacles	(1)
Société pétrolière	(18)
Service d'investissement	(62)
Application de la loi, mise en liberté surveillée, libération sur parole	(11)
Bien-être social et prestations	(38)
Enregistrement des hypothèques sur les biens meubles	(1)
Échange de renseignements concernant le crédit	(7)
Industrie de service	(79)
Employeurs industriels principaux	(128)
Organisme de réglementation	(7)
Bureau d'emploi	(11)
Recherche sur le marché	(1)
Association (travail, professionnelle)	(92)
Œuvre de charité	(51)
Fournisseur de liste d'adresses	(2)
Enquêteur privé, agence de recouvrement, ajusteur d'assurance	(42)
Autres (précisez)	(188)

3. Tenez-vous des fiches de renseignements sur les individus appartenant aux catégories suivantes ? (Cochez *une* seule réponse dans *chaque catégorie*).

3. A. *Nombre d'employés* (employés à plein temps, actuellement, à tous les niveaux de votre organisme)

$\emptyset$ = 159

1-100	(398)	1,000-5,000	(185)
100-500	(289)	Plus de 5,000	(56)
500-1,000	(136)		

3. B. *Nombre de clients* (par exemple : clients actuels, patients, étudiants, titulaires de polices, membres, etc.)

$\emptyset$ = 48

Aucun	(97)	25,000-100,000	(107)
1-250	(247)	100,000-500,000	(98)
250-2,000	(243)	Plus de 500,000	(49)
2,000-25,000	(326)		

3. C. *Nombre de sujets* (par exemple : clients éventuels; personnes dont on tient une fiche quant au crédit et aux actes criminels; titulaires de permis de conduire et personnes ayant fait enregistrer leur véhicule; sujets de recherche, etc.)

$\emptyset$ = 124

Aucun	(599)	25,000-100,000	(63)
1-2,000	(233)	100,000-500,000	(37)
2,000-25,000	(124)	Plus de 500,000	(35)

3. D. *Nombre de bénéficiaires de renseignements* (par exemple : marchands, établissements de crédit, employeurs éventuels, etc.)

$\emptyset$ = 121

Aucun	(644)	1,000-50,000	(63)
1-500	(349)	Plus de 50,000	(10)
500-1,000	(28)		

4. Votre organisme considère-t-il que les événements hypothétiques ci-après constituent une menace sérieuse quant à la tenue de vos fiches ? (Cochez *une* réponse dans *chaque rangée*)

		Ø	Oui	Non
4. A.	Destruction volontaire (par exemple : un bombardement)	72	(391)	(750)
4. B.	Vol ou modification inautorisée	83	(427)	(703)
4. C.	Interception téléphonique illégale	89	(188)	(937)
4. D.	Négligence ou indiscrétion des employés	66	(528)	(621)

5. A. Cette question porte sur l'emplacement des fiches, des sujets ou des clients, et des bénéficiaires de renseignements. (Cochez *une* seule réponse dans *chaque rangée.*)

	Entièrement à l'intérieur d'une seule province	Entièrement au Canada	Partiellement aux États-Unis	Entièrement aux États-Unis	Ne s'applique pas
5. A.1 Fiches Ø = 27	(771)	(229)	(86)	(5)	(27)
5. A.2 Sujets ou clients Ø = 91	(387)	(334)	(227)	(10)	(166)
5. A.3 Bénéficiaires de renseignements. Ø = 122	(198)	(266)	(172)	(10)	(453)

5. B. Indiquez l'affirmation qui décrit le mieux vos relations de travail avec les fournisseurs de renseignements localisés aux États-Unis (par exemple : les bureaux de crédit, etc.) (Cochez *une* seule réponse dans *chaque rangée.*)

Jamais
À l'occasion
Fréquemment
Nous ne savons pas
Ne s'applique pas

5. B.1 (457) (360) (59) (8) (277)
Nous leur fournissons des renseignements
∅ = 45

5. B.2 (364) (421) (184) (8) (249)
Nous en obtenons des renseignements
∅ = 68

5. C. Avez-vous déjà sérieusement songé à traiter certaines parties de vos données aux États-Unis ?

∅ = 39 Oui (151) Non (1022)

5. D. Dans quelles conditions seriez-vous portés à établir vos dossiers aux États-Unis ? (Cochez *une* seule réponse) ∅ = 56

Les dossiers sont déjà aux États-Unis (57)
À des fins économiques (112)
Pour éviter un sérieux désavantage (109)
Sous aucun prétexte actuellement prévisible (880)

6. A. Étant donné votre compréhension de l'équilibre à réaliser entre le besoin pour votre organisation de rassembler des renseignements et l'intérêt de l'individu, en ce qui concerne le caractère confidentiel de sa fiche, indiquez quelle affirmation (*a* ou *b*) de chaque groupe s'applique le mieux. (Cochez *une* seule réponse dans *chaque paire*)

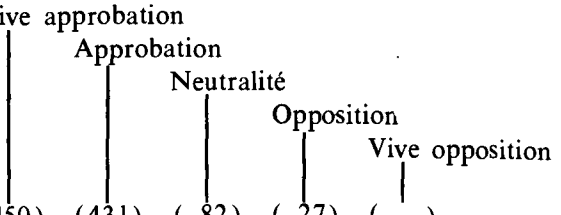
6. A.1 a) Notre organisme a besoin de nouvelles règles plus détaillées régissant le rassemblement et l'utilisation des données personnelles. ∅ = 39 (242)

b) Nos règles et pratiques actuelles sont satisfaisantes. (931)

6. A.2 a) Nous avons besoin de garanties matérielles supplémentaires en ce qui a trait au rassemblement, à l'emmagasinage et à la distribution des renseignements permettant d'identifier les sujets individuellement Ø = 43 (229)

b) Nos garanties matérielles sont maintenant suffisantes (942)

6. B. Les sujets sur lesquels nous tenons des fiches contenant des renseignements permettant de les identifier individuellement devraient avoir les droits suivants (Cochez *une* réponse dans *chaque rangée.*)



6. B.1 (450) (431) (82) (27) ( )
Être mis au courant de l'existence de telles fiches au moment où elles sont entreprises.
Ø = 78

6. B.2 (330) (421) (121) (186) (91)
Prendre connaissance, sur demande, du contenu des fiches qui les concernent.
Ø = 66

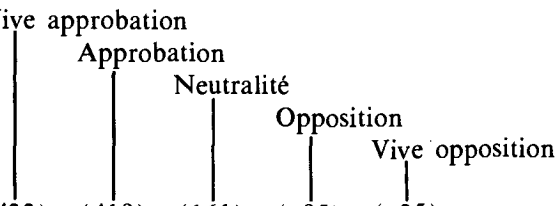
6. B.3 (422) (478) (97) (88) (52)
Mettre à jour, corriger et rayer l'information désuète ou fausse, ou même démontrer la fausseté de certaines données qui les concernent.
Ø = 78

6. B.4 (202) (243) (257) (327) (109)
Recevoir périodiquement un compte rendu de l'usage fait de l'information qui les regarde.
Ø = 77

6. B.5 (232) (357) (193) (244) (113)
Connaître les sources de l'information qui les concerne.
$\emptyset$ = 76

6. B.6 (232) (211) (207) (344) (139)
Mettre fin à l'échange de renseignements sur leur compte, entre les fournisseurs d'information.
$\emptyset$ = 82

6. C. Les mesures ci-après concernant les banques de données qui possèdent des données sur des personnes identifiables sont nécessaires. (Cochez *une* seule réponse dans *chaque rangée*)



6. C.1 (422) (419) (161) (95) (25)
L'enregistrement du but poursuivi et du contenu.
$\emptyset$ = 93

6. C.2 (368) (440) (206) (58) (23)
Des normes de sécurité en matière de matériel et de périgramme.
$\emptyset$ = 120

6. C.3 (435) (461) (143) (49) (24)
Normes au sujet de l'acquisition et de la diffusion de l'information
$\emptyset$ = 103

6. C.4 (291) (391) (275) (99) (51)
Faire sur place des inspections périodiques.
$\emptyset$ = 108

6. D. Les personnes ci-après et les organismes qui font le commerce de l'information d'ordre personnel devraient être licenciés et certifiés. (Cochez *une* seule réponse dans *chaque rangée.*)

Vive approbation | Approbation | Neutralité | Opposition | Vive opposition

6. D.1 (592) (362) (112) (44) (19)
Propriétaires de banques de données
Ø = 86

6. D.2 (606) (356) (114) (33) (16)
Courtiers en information (fournisseurs)
Ø = 90

6. D.3 (479) (346) (188) (86) (35)
Centres de traitement des données
Ø = 89

6. D.4 (376) (255) (265) (176) (52)
Programmeurs d'ordinateur
Ø = 91

6. D.5 (446) (336) (205) (101) (39)
Assembleurs de données
Ø = 88

6. E. Veuillez ne cocher qu'*une* seule réponse par *rangée* :

Vive approbation | Approbation | Neutralité | Opposition | Vive opposition

6. E.1 (93) (189) (107) (433) (325)
Les fiches sont la propriété exclusive des propriétaires de systèmes d'information ; les sujets n'y ont pas d'intérêt.
Ø = 68

6. E.2 (123) (351) (158) (286) (225)
Les propriétaires de systèmes d'information

devraient fournir des données d'ordre personnel aux agents de la loi qui le demandent.
Ø = 72

6. E.3 (395) (585) (82) (60) (26)
On devrait éliminer périodiquement l'information désuète des dossiers.

Section 2

Du n° 7 au n° 14, les questions se rapportent au dossier de fiches dont il est fait mention dans la lettre d'accompagnement. Veuillez répondre à ces questions en vous en tenant aux renseignements qui concernent ce dossier seulement.

7. *Classification du dossier.* Veuillez cocher *la* réponse qui caractérise le mieux le dossier au sujet duquel vous fournissez les renseignements. Ø = 64

Vos propres employés	(352)
Clients	(633)
Sujets	(165)

8. A. Indiquez le nombre approximatif d'individus sur lesquels vous tenez des fiches dans ce dossier.
(Cochez *une* seule réponse) Ø = 62

1-5 000	(694)	50 000-500 000	(178)
5 000-50 000	(228)	Plus de 500 000	(53)

8. B. Indiquez le nombre approximatif de caractères (multiples) d'une fiche individuelle de ce dossier.
(Cochez *une* seule réponse) Ø = 253

1-300	(601)	700-2 000	(109)
300-700	(162)	Plus de 2 000	(90)

8. C. Indiquez la langue de mise en mémoire des fiches.
(Cochez *une* seule réponse) Ø = 51

Anglais	(882)	Les deux langues officielles	(118)
Français	(77)	Codée	(87)

9. Mettez-vous à la disposition de personnes ou d'organismes autres que le vôtre des renseignements de ce dossier, permettant d'identifier un individu ? (sauf tel qu'exigé en vertu de la loi fédérale ou provinciale) :

∅ = 48 Oui (449) Non (718)

10. A. Comment donnez-vous aux bénéficiaires de renseignements les renseignements de ce dossier, permettant d'identifier un individu ? (Cochez *une* seule réponse dans chaque rangée.)

	Jamais	À l'occasion	Fréquemment	Nous ne savons pas	Ne s'applique pas
10. A.1 Nous publions périodiquement des rapports généraux ∅ = 84	(660)	(106)	(82)	(4)	(279)
10. A.2 Nous distribuons des rapports spéciaux de manière sélective ∅ = 90	(502)	(267)	(112)	(9)	(235)
10. A.3 Nous donnons les renseignements en réponse à des demandes précises ∅ = 56	(172)	(600)	(268)	(7)	(112)

10. B. Indiquez le nombre moyen approximatif de demandes précises auxquelles vous répondez chaque année. (Cochez *une* seule réponse.)
∅ = 66

Aucune	(270)	1 000-10 000	(98)
1-100	(524)	Plus de 10 000	(44)
100-1 000	(221)		

11. A. Avez-vous des principes généraux de conduite au sujet de la divulgation des renseignements permettant d'identifier un individu ? (Cochez *une* seule réponse). ∅ = 48

Nous n'avons formulé aucune ligne de conduite (138)
Oui, nous avons une ligne de conduite non écrite (646)
Oui, nous avons une ligne de conduite écrite (383)

11. B. Avez-vous exposé clairement cette ligne de conduite aux groupes suivants ? (Cochez *une* seule réponse dans *chaque rangée.*)

	Nous ne l'avons presque jamais communiquée	Nous en discutons quand le besoin se fait sentir	Nous l'avons régulièrement communiquée	Ne s'applique pas
11. B.1 Individu dont vous tenez des fiches dans ce dossier. ∅ = 66	(247)	(594)	(72)	(235)
11. B.2 Préposés à la tenue des fiches ∅ = 66	(46)	(377)	(566)	(159)
11. B.3 Public général ∅ = 73	(243)	(215)	(35)	(647)

11. C. Avez-vous un régime de discipline au cas où vos propres employés violeraient le caractère confidentiel de ces fiches ? (Cochez *une* seule réponse.) ∅ = 69

Nous ne surveillons pas les démarches de nos employés. (269)

Nous surveillons les démarches de nos employés et nous n'avons jamais eu connaissance de

manquements quant au caractère confidentiel des fiches. (763)

Nous surveillons les démarches de nos employés et nous réprimons sévèrement les manquements quant au caractère confidentiel des fiches dès que de tels manquements sont constatés. (114)

11. D. Existe-t-il différentes dispositions concernant la divulgation qui sont jointes à diverses portions des fiches de ce dossier ?

∅ = 67 Oui (361) Non (787)

11. E. Les individus dont vous tenez des fiches dans ce dossier ou des groupes désignés expressément pour défendre leurs intérêts se sont-ils déjà plaints au sujet de la divulgation de renseignements contenus dans ce dossier à des personnes extérieures à votre organisme ? (Cochez *une* seule réponse dans *chaque rangée.*) ∅ = 47

Jamais	(873)
À l'occasion	(121)
Fréquemment	(4)
Nous ne savons pas	(135)
Ne s'applique pas	(35)

12. A. En règle générale, un individu peut-il examiner sa propre fiche du dossier, ou une copie ? (Cochez *une* seule réponse.) ∅ = 64

L'individu ne sait pas que la fiche existe	(63)
Il ne peut comprendre les données contenues dans sa fiche	(134)
Il peut examiner *toutes les données* de sa fiche	(499)
Il peut examiner *certaines données* de sa fiche	(282)
Il ne peut examiner *aucune donnée* de sa fiche	(173)

12. B. Si un individu a l'autorisation d'examiner des données de sa fiche, assurez-vous une traduction ou une interprétation dans une langue que comprend l'individu ?

∅ = 260 Oui (649) Non (304)

12. C. Des individus ou des groupes désignés pour défendre les intérêts de ces derniers ont-ils déjà cherché à examiner leurs propres fiches ou se sont-ils déjà plaints des pratiques de votre organisme, en ce qui a trait au droit qu'a l'individu d'examiner les fiches qui le concernent ? (Cochez *une* seule réponse.) Ø = 56

Jamais	(862)
À l'occasion	(190)
Fréquemment	(8)
Nous ne savons pas	(61)
Ne s'applique pas	(38)

13. A. Indiquez quel moyen vous avez employé pour rassembler les renseignements inclus dans ce dossier ? (Cochez *une* seule réponse dans chaque rangée.)

	Aucun	Certains	La plupart	Tous
13. A.1 Autres fournisseurs de renseignements Ø = 133	(451)	(530)	(67)	(34)
13. A.2 Publications ou fiches publiques Ø = 144	(744)	(288)	(26)	(13)
13. A.3 Individu sur lequel vous tenez une fiche Ø = 78	(63)	(211)	(474)	(396)
13. A.4 Bénéficiaires de renseignements (par exemple : marchands) Ø = 139	(819)	(212)	(33)	(12)
13. A.5 Enquêteurs Ø = 130	(745)	(264)	(48)	(28)

13. B. Des individus ou des groupes désignés pour défendre les intérêts de ces derniers se sont-ils déjà plaints des moyens employés pour obtenir quelque renseignements que ce soit pour ce dossier ? (Cochez *une* seule réponse.) Ø = 46

Jamais	(903)
À l'occasion	(159)
Fréquemment	(5)
Nous ne savons pas	(69)
Ne s'applique pas	(32)

13. C. Indiquez si les sources ci-après sont utilisées pour rassembler l'information sur des personnes identifiées dans le but de la conserver dans vos dossiers. (Cochez *une* seule réponse dans *chaque rangée*). Ø = 48

	Jamais utilisée	Quelquefois utilisée	Généralement utilisée	Toujours utilisée	Ne s'applique pas
13. C.1 Le sujet lui-même Ø = 48	(30)	(109)	(288)	(711)	(37)
13. C.2 Les membres de la famille du sujet Ø = 71	(454)	(448)	(98)	(27)	(116)
13. C.3 Les voisins ou les amis du sujet Ø = 77	(641)	(318)	(22)	(9)	(149)
13. C.4 Certaines personnes nommées par le sujet Ø = 73	(220)	(482)	(203)	(102)	(135)
13. C.5 Les employeurs précédents du sujet Ø = 77	(304)	(413)	(176)	(78)	(167)

13. C.6 (298) (396) (126) (89) (226)
L'employeur actuel
$\emptyset$ = 80

13. C.7 (352) (310) (167) (168) (151)
Médecins et hôpitaux
$\emptyset$ = 67

13. C.8 (574) (299) (25) (18) (226)
Agences d'application des lois
$\emptyset$ = 72

13. C.9 (378) (386) (119) (81) (186)
Écoles fréquentées par le sujet
$\emptyset$ = 72

13. D. Indiquez lesquelles des techniques ci-après sont utilisées par vos représentants pour rassembler l'information sur des personnes identifiées pour la mettre en mémoire dans vos dossiers. (Cochez *une* seule réponse dans *chaque rangée.*)

Jamais utilisée
Quelquefois utilisée
Généralement utilisée
Toujours utilisée
Ne s'applique pas

13. D.1 (93) (95) (211) (420) (317)
Le représentant s'identifie lui-même à l'aide de documents probants
$\emptyset$ = 79

13. D.2 (122) (110) (167) (360) (362)
Il identifie son employeur
$\emptyset$ = 94

13. D.3 (116) (107) (154) (372) (372)
Il donne la raison de son enquête
$\emptyset$ = 94

13. D.4 (162) (87) (96) (250) (524)
Il promet de protéger l'informateur
$\emptyset$ = 96

13. D.5 (177) (68) (95) (255) (516)
Il garantit que l'information sera utilisée à bon escient.
$\emptyset$ = 104

13. D.6 (140) (142) (147) (252) (434)
Il prouve que le sujet a accepté de fournir les renseignements qui le concernent.
$\emptyset$ = 99

13. D.7 (161) (244) (149) (85) (476)
Il confirme des faits d'au moins deux sources indépendantes.
$\emptyset$ = 100

14. A Quand un individu dont vous tenez des fiches se voit refuser l'aide qu'il requérait ou rompt ses liens avec votre organisme, pendant combien de temps sa fiche est-elle mise en mémoire ? (Cochez *une* seule réponse.) $\emptyset$ = 55

La fiche est éliminée immédiatement	(55)
Elle est retenue jusqu'à 18 mois	(94)
Elle est retenue entre 18 mois et 7 ans	(301)
Elle est retenue pour une période de 7 ans ou plus	(540)
Nous ne savons pas	(60)
Ne s'applique pas	(110)

14. B. Quand les fiches sont éliminées de ce dossier, quel usage en fait-on ? (Cochez *une* seule réponse.)
$\emptyset$ = 50

Elles sont détruites	(549)
Elles sont renvoyées à l'individu qu'elles concernaient	(4)
Elles sont transférées à un dossier inactif	(271)
Elles sont transférées à un système d'archives	(161)
Nous ne savons pas	(26)
Ne s'applique pas	(154)

14. C. Quel usage fait-on du dossier conservé de l'individu auquel on refuse l'aide qu'il requérait ou qui rompt ses liens avec votre organisme (y compris les dossiers inactifs et ceux servant aux archives). (Cochez *une* seule réponse.) $\emptyset = 67$

Ces dossiers ne sont pas consultés	(269)
Ils sont utilisés pour vérifier les nouvelles demandes présentées à notre organisme	(258)
Les données contenues dans ces dossiers sont envoyées à l'entrepôt principal	(55)
Les renseignements sont échangés avec d'autres organismes	(105)
Nous ne savons pas	(45)
Ne s'applique pas	(416)

Section 3

Les questions ci-après (15-22) se rapportent à l'utilisation d'ordinateurs ou de services d'informatique sans se référer à un dossier en particulier. Si vous n'utilisez pas de système d'ordinateur, veuillez vous arrêtez ici et nous retourner le questionnaire dès que vous le pourrez. Nous vous sommes reconnaissants d'avoir bien voulu collaborer avec nous.

15. A. Quand avez-vous, pour la première fois, utilisé un système d'ordinateur pour emmagasiner et traiter des fiches ? (Cochez *une* seule réponse.) $\emptyset = 691$

Avant 1955	(23)	1964-1969	(265)
1955-1960	(51)	Après 1969	(81)
1960-1964	(102)		

15. B. Quand votre processeur central actuel a-t-il été établi ? (Répondez en fonction de votre ordinateur principal utilisé pour le traitement des fiches.) (Cochez *une* seule réponse.) $\emptyset = 689$

Avant 1964	(34)	Ne s'applique pas	(122)
Entre 1964 et 1969	(240)		
Après 1969	(130)		

15. C. Quelle est la capacité de mise en mémoire de votre processeur central, en nombre de mots d'ordinateur ? (Cochez *une* seule réponse.) $\emptyset = 714$

Moins de 64 000 (156)
Entre 64 000 et 256 000 (145)
Plus de 256 000 (65)
Ne s'applique pas (135)

15. D. Quelle est la capacité de mise en mémoire intermédiaire pour utilisation directe de votre ordinateur, en nombre de caractères (multiplets) ? (Cochez *une* seule réponse.) $\emptyset = 723$

Moins de 100 millions (164)
Entre 100 et 200 millions (65)
Plus de 200 millions (56)
Ne s'applique pas (207)

16. A. Tenez-vous des fiches emmagasinées dans un ordinateur sur certains (aucun, quelques-uns, la plupart ou la totalité) de vos employés, clients et sujets ? (Cochez *une* réponse dans *chaque rangée.*)

	Aucun	Quelques-uns	La plupart	Tous	Ne s'applique pas
16. A.1 Employés $\emptyset = 701$	(145)	(57)	(62)	(218)	(32)
16. A.2 Clients $\emptyset = 700$	(50)	(79)	(88)	(249)	(49)

16. A.3 (122) (59) (31) (45) (235)
Sujets
∅ = 73

16. B. Sur la totalité des renseignements que vous possédez sur chaque employé, client ou sujet, combien sont *emmagasinés dans un ordinateur* ? (Cochez *une* seule réponse dans *chaque rangée.*)

Aucun renseignement
Quelques renseignements
La plupart des renseignements
Tous les renseignements
Ne s'applique pas

16. B.1 (125) (203) (121) (20) (50)
Employés
∅ = 696

16. B.2 (39) (236) (141) (43) (58)
Clients
∅ = 698

16. B.3 (103) (85) (38) (14) (251)
Sujets
∅ = 724

17. A. Quel a été l'effet *principal* sur votre organisme, de l'emploi de l'ordinateur pour traiter ces dossiers ? (Cochez *une* seule réponse.) ∅ = 691

Amélioration dans les manœuvres de routine et de grandes dimensions (241)
Les rapports parviennent à la gestion plus à temps et sont plus complets (213)
Nette amélioration dans le travail de planification des politiques (18)
Aucun terme de comparaison (51)

17 B. Laquelle des affirmations ci-après décrit *le mieux* votre expérience des applications du traitement des données par ordinateur ? (Cochez *une* seule réponse.) ∅ = 689

Nous ne pourrions pas tenir des dossiers d'une dimension et d'une complexité telles que les nôtres sans un ordinateur (228)
L'utilisation de l'ordinateur nous a aidé à tenir les dossiers, mais nous pourrions continuer de le faire sans utiliser un ordinateur (251)
L'ordinateur nous a relativement peu aidé à tenir nos dossiers (20)
Aucun terme de comparaison (26)

18. Qui, en général, exploite le système d'ordinateur aux fins de traitement des fiches renfermant des renseignements permettant d'identifier un individu ? (Cochez *une* seule réponse.) ∅ = 694

Nous avons notre propre système d'ordinateur sur les lieux (314)
Nous utilisons les services d'un bureau ou d'une autre installation d'ordinateur, à l'extérieur de notre organisme (205)

19. A. Le fait d'emmagasiner ces fiches dans un ordinateur a-t-il conduit à la détection et à la correction d'erreurs réelles qui existaient auparavant dans les fiches ? (Cochez *une* seule réponse.)

∅ = 688 Oui (301) Non (105)
Nous ne savons pas (73)
Ne s'applique pas (47)

19. B. Les corrections étaient-elles importantes du point de vue des décisions à prendre sur les personnes qui faisaient l'objet de fiches ? (Veuillez ne cocher qu'*une* seule réponse.) ∅ = 690

Oui, très importantes (52)
Oui, mais d'une importance marginale (122)
Non, presque pas ou pas du tout importantes (122)
Aucune idée (50)
Ne s'applique pas (178)

19. C. Avez-vous affronté de nouvelles difficultés dans votre effort pour garder les fiches exactes, depuis l'emploi de l'ordinateur ? ∅ = 685

Oui, de sérieuses difficultés (25)
Oui, des difficultés marginales (123)
Non, des problèmes mineurs ou pas de problèmes du tout (332)
Aucune idée (22)
Ne s'applique pas (28)

20. A. Une série de mesures ont été proposées pour empêcher que des personnes non autorisées ne prennent connaissance des fiches mises en ordinateur. Utilisez-vous quelques-unes de celles que nous énonçons ci-dessous ? (Cochez *une* seule réponse dans *chaque rangée.*)

		Ø	Oui	Non
20. A.1	Contrôle préventif de l'accès au dossier (par exemple, des verrous aux portes, cartes spéciales que doivent porter ceux qui ont accès à l'ordinateur)	739	(343)	(132)
20. A.2	Des mesures de sécurité en matière de matériel ou de périgramme (comme les mots de passe, le code d'identification du terminal, le codage cryptographique)	750	(180)	(283)
20. A.3	Des vérifications concernant l'intégrité du personnel (par exemple, enquêtes spéciales sur les personnes qui travaillent au dossier; employés faisant l'objet d'une police d'assurance spéciale)	745	(197)	(271)
20. A.4	Journaux de vérification ou autres méthodes de contrôle des données	754	(264)	(194)
20. A.5	Des procédures et des règlements concernant l'élimination des données (par exemple, la destruction des imprimés ou des rubans)	745	(323)	(147)
20. A.6	Autres, veuillez préciser	950	(31)	(232)

20. B. Combien de terminaux à distance, à grande vitesse, mis à part les terminaux à clavier (par exemple, lecteur de cartes) sont utilisés dans votre système ? (Cochez *une* seule réponse.) $\emptyset$ = 743

Aucun	(348)	plus de 6	(22)
de 1 à 6	(102)		

20. C. Combien de terminaux à distance, à clavier, sont utilisés dans votre système ? (Cochez *une* seule réponse.) $\emptyset$ = 743

Aucun	(338)	de 12 à 200	(26)
de 1 à 12	(101)	plus de 200	(7)

20. D. Veuillez indiquer la description qui caractérise le mieux vos opérations de télétraitement des données. (Ne cochez qu'*une* seule réponse dans *chaque rangée.*)

	Aucun	Entrée de données seulement	Affichage de l'information seulement	Entrée et sortie
20. D.1 Terminaux à distance, à grande vitesse (par exemple, lecteur de cartes, imprimante) $\emptyset$ = 744	(353)	(10)	(5)	(103)
20. D.2 Terminaux à distance, à clavier (par exemple, téléimprimeurs, représentation par image) $\emptyset$ = 749	(352)	(18)	(15)	(81)

21. L'application des techniques de l'ordinateur, dans votre organisme, vous permet-elle de réunir en un seul dossier toute l'information que votre organisme rassemble et met en fiche sur une personne donnée ?

$\emptyset$ = 694 Oui (148) Non (313)
Ne s'applique pas (60)

22. A. Fournissez-vous plus d'*information sur des personnes identifiables* à des organismes gouvernementaux (fédéraux, provinciaux ou municipaux) à la suite de l'emploi d'un ordinateur et d'une capacité accrue de retrouver l'information ?

$\emptyset$ = 694 Oui (69) Non (369)
Ne s'applique pas (82)

22. B. Fournissez-vous un plus grand nombre de données *statistiques* sur des personnes non identifiables à des organismes gouvernementaux à la suite de l'emploi d'un ordinateur et d'une capacité accrue de retrouver l'information ?

$\emptyset$ = 695 Oui (151) Non (297)
Ne s'applique pas (71)

Section 4

Les questions ci-après se rapportent aux fiches mises en mémoire par ordinateur et qui font partie du dossier dont il est fait mention dans la lettre d'accompagnement. Si vous n'utilisez *pas* de système d'ordinateur pour ce dossier, veuillez vous arrêter ici et nous retourner le questionnaire dès que vous le pourrez. Nous vous sommes reconnaissants d'avoir bien voulu collaborer avec nous.

23. A. En ce qui a trait à ce dossier, rassemblez-vous plus de données ou moins de données sur une personne en particulier que vous ne le faisiez avant d'utiliser l'ordinateur ? (Veuillez ne cocher qu'*une* seule réponse.) $\emptyset$ = 791

Plus de données par personne (147)
Environ la même quantité de données par personne (242)
Moins de données par personne (6)
Aucun terme de comparaison (28)

23. B. L'usage de l'ordinateur a-t-il influencé directement la quantité de données par fiche ? $\emptyset$ = 791

Oui (158) Non (247)
Ne s'applique pas (19)

23. C. À laquelle des deux explications ci-après devez-vous en tout premier lieu l'accroissement de données ? (Veuillez ne cocher qu'*une* seule réponse.) ∅ = 798

À la capacité accrue de l'ordinateur d'emmagasiner et de traiter (89)
Aux changements dans les objectifs ou programmes structurels ou aux besoins accrus des gouvernements de rassembler ou de faire connaître l'information (131)
Ne s'applique pas (197)

24. A. Pour ce qui est des personnes sur lesquelles vous faites des fiches dans ce dossier, tenez-vous d'autres renseignements que vous traitez manuellement ?

∅ = 791 Oui (380) Non (43)

24. B. Quelle comparaison feriez-vous entre l'information traitée à l'ordinateur et celle qui est traitée manuellement ? (Cochez *une* seule réponse dans chaque rangée.)

		∅	Oui	Non
24. B.1	L'information subjective (fondée sur des opinions) est encore traitée manuellement	824	(322)	(66)
24. B.2	L'information sous forme de longs exposés ou de graphiques est encore traitée manuellement	817	(345)	(52)
24. B.3	L'information la plus délicate et la plus confidentielle est traitée manuellement	824	(294)	(97)

25. A. Depuis que vous avez commencé à utiliser un système d'ordinateur, de nouvelles règles ont-elles été énoncées en ce qui a trait au droit des personnes à prendre connaissance des fiches qui les concernent dans ce dossier ?

Ø = 790 Oui (14) Non (359)
Ne s'applique pas (52)

25. B. Ce changement vous semble-t-il le résultat *direct* de l'application de l'ordinateur au domaine des fiches ?

Ø = 792 Oui (11) Non (69)
Ne s'applique pas (343)

26. Pensez-vous utiliser autrement les renseignements d'ordre personnel de ce dossier (par exemple, pour vendre des listes d'adresses, préparer des évaluations de marché, etc.)

Ø = 796 Oui (81) Non (336)

Veuillez mentionner les utilisations possibles à l'étude

Nous vous sommes reconnaissants d'avoir bien voulu apporter votre collaboration. Veuillez retourner le questionnaire dans l'enveloppe prévue à cet effet.

LES MÉMOIRES

La communication ci-après a été adressée à 187 associations professionnelles et industrielles canadiennes, les invitant à faire connaître leurs vues dans un mémoire.

Le 26 avril 1971

Le maintien du caractère privé des communications et la protection des droits des particuliers en général préoccupent continuellement les gouvernements et cette préoccupation est particulièrement centrée maintenant sur les problèmes spéciaux qui sont posés par le développement des systèmes d'informatique.

Différents genres d'études sont actuellement en cours dans les autres pays. Au Canada, nos études ont débuté par une conférence sur « L'ordinateur : La vie privée et la liberté d'information » qui s'est tenue en mai dernier à l'Université Queen's, dans le cadre des études de la Télécommission sur les télécommunications. Cette conférence a été organisée sous les auspices des ministères des Communications et de la Justice du Canada, de la Société d'informatique du Canada et de l'Université Queen's. Vous trouverez sous ce pli un exemplaire anticipé du rapport de cette conférence.

L'étape suivante a été l'établissement par le ministère de la Justice et le ministère des Communications d'un Groupe d'étude conjoint sur l'ordinateur et la vie privée afin d'étudier avec plus de détails et en profondeur certains des problèmes et des questions qui ont été soulevés par la conférence. Le mandat du Groupe d'étude est comme il suit :

« D'une manière générale, étudier les droits et les valeurs connexes, liés à l'individu, qu'ils soient actuels ou en voie de se constituer, ainsi que les questions découlant des possibilités d'atteintes à la vie privée par la collecte des données que renferment les systèmes d'information et de classement automatisés, de même que par leur stockage, leur traitement et leur exploitation.

a) déterminer les types d'informations personnelles actuellement stockées, traitées et diffusées, ou qui le seraient dans l'avenir, par le moyen des systèmes

d'information automatisés, tant au gouvernement que dans les organisations de toute nature ;

b) examiner les méthodes et les mécanismes de collecte, de stockage, de traitement et de diffusion des informations d'ordre personnel quant à leurs incidences sur le respect du droit à la vie privée et des droits individuels connexes ;

c) apprécier les techniques de protection visant à prévenir l'accès illicite aux systèmes d'information automatisés ;

d) étudier les mesures d'ordre juridique, réglementaire, technique ou professionnel susceptibles d'assurer le respect du droit à la vie privée et des droits individuels connexes, et apprécier les facteurs commerciaux, juridiques ou constitutionnels qui pourraient en gêner l'application. »

Pour éviter tout malentendu, nous devrions expliquer que le Groupe d'étude sur l'ordinateur et la vie privée est un groupe d'étude séparé du Groupe d'étude sur la téléinformatique au Canada, bien que lui étant complémentaire. Ce dernier groupe d'étude communiquera peut-être avec vous au sujet de questions qui sont directement de son ressort.

L'étude entreprise par le Groupe d'étude sur la vie privée sera très étendue ; elle sera fondée sur les renseignements et les opinions éclairées les plus vastes possible et examinera aussi bien les systèmes d'information manuels que les systèmes automatisés. Un questionnaire sera distribué à un grand nombre de sociétés et d'institutions qui possèdent des systèmes d'information, et un très grand nombre d'entrevues sur les lieux auront lieu, sur une base d'échantillonnage.

Le but de la présente lettre est d'inviter votre association à exprimer son opinion sur les questions générales qui sont du ressort du Groupe d'étude. Nous comprenons bien que la nature et la forme de votre réponse seront guidées par les intérêts de votre association, mais nous espérons que vous vous sentirez libre de présenter des observations sur n'importe quel aspect de la question, que cet aspect soit ou ne soit pas directement en rapport avec les entreprises de vos membres. Certaines des questions qui ont été soulevées au cours d'études sur cette question, entreprises au Canada ou ailleurs, sont celles qui ont trait aux déclarations officielles des exploitants de banques de données concernant leurs objectifs, leur code d'éthique professionnelle, le droit qu'ont les individus d'avoir accès à leurs dossiers, de vérifier l'exactitude de

leur contenu, et d'être informés au sujet de l'utilisation des renseignements contenus dans ces dossiers. Il y a aussi la question des normes techniques susceptibles d'assurer la sécurité des données et des systèmes, et la question de la délivrance de licences aux banques de données. La liste n'est pas complète. Elle pourra, toutefois, vous aider à vous concentrer sur les aspects importants de ce vaste domaine ; en même temps, vous pouvez ignorer n'importe quel sujet ou tous les sujets, et faire des observations sur d'autres questions qui ne sont pas mentionnées.

Nous serions aussi heureux de recevoir directement les observations de tous ceux de vos membres qui désireraient exprimer leur point de vue. Nous comprenons bien entendu que, dans tout groupement, il peut y avoir d'importantes différences d'opinions.

Vous trouverez sous ce pli une carte indiquant l'intention de déposer (ou de ne pas déposer) un mémoire. Nous vous saurions gré de bien vouloir nous la renvoyer aussitôt que possible et de présenter votre mémoire avant la fin du mois de juin.

Veuillez agréer l'expression de mes meilleurs sentiments.

Le Directeur,
Planification socio-économique,
Ministère des Communications,

Richard J. Gwyn

Le Directeur,
Recherche juridique et planification,
Ministère de la Justice,

E. R. Olson

Privacy and Computers Task Force,
P.O. Box 8350,
Ottawa, Canada K1G 3H8

SURVEY REPLY

We intend to participate in the survey the Computers and Privacy Task Force and

☐ will sumit a brief by June 31st, 1971.

☐ do not intend to submit a brief.

Groupe d'étude sur l'ordinateur et la vie privée
C.P. 8350
Ottawa, Canada K1G 3H8

CARTE-RÉPONSE

Nous désirons prendre part à l'enquête du Groupe d'étude sur l'ordinateur et la vie privée :

☐ nous présenterons un mémoire au plus tard le 30 juin 1971.

☐ nous n'avons pas l'intention de présenter un mémoire.

Association name and postal address
Nom et adresse postale de l'association

Name of association's representative
Nom du représentant de l'association

Title
Titre

Telephone No.
N° de téléphone

Postal address
Adresse postale

Le Groupe a reçu des mémoires des organisations suivantes :

Canadian Association of Data Processing Service Organizations
Association des banquiers canadiens
Canadian Book Publishers' Council
Association canadienne des fabricants d'équipement de bureau
Canadian Copyright Institute
Association canadienne des compagnies d'assurance-vie
Association des manufacturiers canadiens
Association médicale canadienne
Clarke Institute of Psychiatry
Committee of Presidents of Universities of Ontario
Ontario Medical Association
Retail Council of Canada
Retail Credit Company of Canada Limited
Banque royale du Canada
Association du téléphone du Canada
United Community Fund of Greater Toronto

Par ailleurs, le Groupe d'étude sur la téléinformatique au Canada, du ministère des Communications, a reçu 54 mémoires où était abordée la question de la vie privée.

Banques d'information étrangères

À notre demande, les organisations suivantes exploitant des banques d'information où sont stockées des données personnelles sur des Canadiens, nous ont fait tenir les renseignements désirés sur leurs pratiques à cet égard :

American Airlines Inc.
American Express
Carte Blanche
Diners Club Inc.
Hooper Holmes Bureau Inc. – Credit Index
– Casualty Index
ITT Data Processing
Institute of Electrical and Electronics Engineers
McGraw-Hill Data Service
National Data Corp.
Recording and Statistical Corp. – Medical Information Bureau
Retail Credit Corp.
TRW Inc. – Credit Data Corp.

Bibliographie

Certains chercheurs voudront peut-être prendre connaissance de la documentation et des ouvrages de référence utilisés par le Groupe d'étude. Parmi les nombreux ouvrages que nous nous sommes procurés, nous estimons que les suivants offrent une bibliographie exhaustive.

HARRISON, Anette
« The Problem of Privacy in the Computer Age : An annotated Bibliography. »
Santa Monica, The RAND Corporation, 1970. Mise à jour d'une étude antérieure effectuée à la demande du gouvernement des États-Unis (2 volumes). C'est la bibliographie la plus complète qui soit sur le sujet.

MILLER, Arthur R.
« Assault on Privacy »
Ann Arbor : University of Michigan Press, 1971, Bibliographie (pp. 261 à 269) comportant environ 200 références classées.

United States, House of Representatives, Subcommittee of the Committee on Government Operations, 89th Congress.
« The Computer and Invasions of Privacy »
Washington : U.S. Government Printing Office, 1966 ;
New York : Arno Press, 1967.
« Letters, statements, etc, submitted for the record... », pp. 135 à 311. Traite essentiellement des pratiques du gouvernement des États-Unis en matière d'information personnelle (vie privée).

WESTIN, Alan F.
« Privacy and Freedom »
New York, Atheneum, 1970
bibliographie : pp. 445 à 458. Environ 440 références classées sous quatre rubriques.

YOUNGER, Rt. Hon. Kenneth (Président)
« Report of the Committee on Privacy »
London : Her Majesty's Stationery Office, juillet 1972, (Cmnd. 5012).
Appendice C, « Select Bibliography », pp. 223-224.

Études similaires

Des études sur l'information et la vie privée ont été effectuées ou sont en cours dans bon nombre d'autres pays, notamment :

Le Danemark

Études faites par le ministère de la Justice.

La France

Le Conseil d'État a mis en œuvre une étude interne. Le rapport n'en a pas encore été publié.

L'Allemagne de l'Ouest

Outre l'étude effectuée pour le compte du ministère de la Justice, un certain nombre d'États examinent la solution adoptée par l'État de Hesse, à savoir la création du poste de Commissaire aux données.

Les Pays-Bas

Le Gouvernement a créé, par le décret royal du 18 février 1972, le « Comité national d'enquête sur la vie privée ». Aucune date de publication n'a été annoncée jusqu'à présent.

La Norvège

L'institut de Droit privé de l'Université d'Oslo, en Norvège, fait une étude pour le ministère de la Justice. Mentionnons également le rapport du Premier Symposium d'Oslo sur les Banques d'information et la société.

L'O.C.D.E.

Le Comité sur le contrôle des données, un sous-groupe de la Commission sur la politique scientifique, a publié en mars 1971 un rapport intitulé : « L'Information numérique et la vie privée ».

La Suède

L'Agence suédoise pour le développement administratif (S.A.F.A.D.) a publié un rapport sur la question de la vie privée intitulé « Data Och Integritet (Information et Intégrité) en juin 1972. On peut se procurer l'édition anglaise abrégée, de 20 pages,

qui est intitulée « Computers and Privacy », à l'adresse suivante : P.O. Box 2106, S-103 Stockholm.

La Suisse

Un groupe spécial du Gouvernement étudie la question.

Le Royaume-Uni

Le *Committee on Privacy*, présidé par le Rt. Hon. Kenneth Younger, a publié son rapport le 12 juillet 1972. On peut se procurer ce volume de 350 pages – qui couvre tous les aspects du problème de la vie privée, y compris ceux qui se rattachent à l'exploitation des banques d'information – en s'adressant au « *Her Majesty's Stationery Office* » (Cmnd. 5013). Prix $ 2.00.

La *British Computer Society* s'est mise à l'étude de la question au début de 1972 ; elle examine avec une attention particulière les possibilités d'établir un code de déontologie.

On s'attend que le groupe d'étude du *British Civil Service* publie un rapport en 1972. Aucune date n'a été annoncée.

Les États-Unis

La publication du rapport de l'Académie nationale des sciences (établi sous la direction d'Alan Westin), est prévue pour l'automne 1972. L'étude, subventionnée par la *Russell Sage Foundation*, a commencé au début de 1970. Une étude a été entreprise au début de 1972 par la *National Science Foundation :* la direction en est confiée au Professeur Arthur Miller. Le rapport du *Decennial Census Review Committee,* publié en juillet 1971, examine les aspects de la question de la vie privée et du caractère confidentiel de l'information personnelle qui sont liés au recensement. Un comité, institué par le *Department of Health, Education and Welfare*, a commencé à tenir des audiences publiques en avril 1972. Son rapport préliminaire serait rendu public le 1 ^{er} janvier 1973. Voir aussi les comptes rendus du *Senate Sub-Committee on Constitutional Rights*, présidé par le Sénateur Sam Erwin.

Index