Gouvernement du Canada
Ministère des Communications

Government of Canada
Department of Communications

QUEEN
KE
5325
.K6614
1987
c.2

Le Centre canadien de recherche sur l'informatisation du travail

Canadian Workplace Automation Research Centre

QUESTIONS DE DROIT QUE POSENT LES SYSTEMES INFORMATIQUES INTEGRES:

APERÇU DES CONSIDERATIONS PRATIQUES ET DES RECENTS DEVELOPPEMENTS DANS CE DOMAINE

par Dr. Jake V. Th. Knoppers
Chercheur principal invité

KE
5325
K661
1987
c.2

Canada

Industry Canada
LIBRARY
JUL 1 3 1998
BIBLIOTHÈQUE
Industrie Canada

QUESTIONS DE DROIT QUE POSENT LES SYSTEMES INFORMATIQUES INTEGRES:

APERÇU DES CONSIDERATIONS PRATIQUES ET DES RECENTS DEVELOPPEMENTS DANS CE DOMAINE

par Dr. Jake V. Th. Knoppers
Chercheur principal invité

Centre canadien de recherche sur l'informatisation du travail

COMMUNICATIONS CANADA
FEB 1 1991
LIBRARY – BIBLIOTHÈQUE

Ce document, fut élaboré pour le Carrefour international sur l'information électronique. Montréal, juin 1987. Les opinions exprimées dans ce rapport n'engagent que l'auteur.

MCC-CCRIT-87-F-C04

DD 7350818
DL 10270938

KE
5325
K66f
1987
c.2

90-05467/1

Sommaire

Auparavant, et même maintenant dans une large mesure, l'information enregistrée était gérée et utilisée sous forme de support papier. L'avènement des nouvelles technologies de l'informatique, les efforts déployés ces dernières années pour leur intégration et pour la réalisation d'un bureau automatisé (sans papier) ont mis en évidence un certain nombre d'importantes questions de droit. Il serait judicieux que les informaticiens se mettent au courant de ces questions et apprennent comment les traiter, aussi bien du point de vue professionnel que du point de vue de l'intégration de ces considérations à leur méthodologie d'élaboration des systèmes. Le secteur de la bureautique pose un défi particulier, parce qu'il vient à peine d'atteindre le stade de l'intégration et parce qu'il a toujours compté énormément sur le papier.

Note aux lecteurs :

L'auteur serait heureux de recevoir des remarques, des critiques et des suggestions au sujet du présent document de recherche. De même, les personnes désireuses de se renseigner sur d'autres recherches dans ce domaine ou de participer à ce programme de recherches sont priées de communiquer avec l'auteur.

TABLE DES MATIÈRES

PAGE

1.0 INTRODUCTION 1

2.0 LOIS SUR L'INFORMATION 3

2.1 Définition 3

2.1.1 Informations enregistrées 4

2.1.2 Manipulation de l'information 4

2.1.3 Lois sur l'information 5

2.2 Récents développements de la législation canadienne sur l'accès à l'information 7

2.2.1 Code criminel 8

2.2.2 Loi sur la preuve au Canada 15

2.2.3 Loi sur l'accès à l'information et Loi sur la protection des renseignements personnels 20

2.2.4 Exigences relatives à la conservation des documents .. 21

2.2.5 Droit d'auteur 22

3.0 CONSIDÉRATIONS PRATIQUES 24

3.1 Définition de "document" : de l'objet à l'information 24

3.2 Protection de l'information enregistrée 26

3.3 Intégrité des données 27

3.4 Stockage des données et des documents électroniques 29

4.0 CONCLUSIONS 31

NOTES BIBLIOGRAPHIQUES 32

1.0 INTRODUCTION

Jusqu'à ces derniers temps, la gestion et l'utilisation de l'information consistaient essentiellement dans la gestion et l'utilisation d'objets physiques sur lesquels l'information était enregistrée de façon permanente. En d'autres termes, il existait un rapport biunivoque entre l'information enregistrée et le support physique. De plus, l'unité indivisible que formaient l'information enregistrée et le support physique n'était pas réutilisable. En réalité, la gestion de l'information était, et le demeure encore aujourd'hui dans une large mesure, surtout dans les bureaux, la gestion d'objets (soit les documents).

Un grand nombre de lois et de principes de jurisprudence, adoptés au cours des siècles, et qui traitent directement de divers aspects de l'information enregistrée, sont propres à une technologie, c'est-à-dire directement liés à des formes particulières d'enregistrement des informations ainsi qu'aux moyens et méthodes de diffusion de ces informations. L'avènement des technologies du traitement de l'information "sans papier" et de communications, conjugué avec leur récente intégration, a donné lieu à une situation où la plus grande partie de la législation sur l'information traditionnelle ne s'applique plus. Même lorsque cette législation s'applique, les informaticiens ne sont pas au courant des exigences que stipulent ces lois et, s'ils le sont, ignorent comment incorporer ces exigences juridiques dans leurs systèmes informatiques intégrés, c'est-à-dire leurs systèmes d'information de gestion et, surtout, les systèmes bureautiques intégrés qu'ils mettent au point.

La présente étude comprend trois sections. La première présente et développe la notion de loi sur l'information. La deuxième indique un certain nombre de lois importantes sur l'information et traite de leur pertinence ainsi que des modifications qui y ont été apportées récemment. La troisième expose certaines considérations pratiques et les questions qu'il faudra résoudre.

Cette étude porte sur les questions de droit, donc de gestion et d'exploitation, qu'implique l'utilisation croissante que nous faisons des technologies de l'information ainsi que sur toute autre barrière non technique qui les empêcherait de devenir les principaux systèmes de soutien opérationnel d'une organisation.

En d'autres termes, il est vrai que les technologies de l'information sont accessibles, à un prix convenable et avec les fonctions appropriées, et que les gestionnaires sont disposés à acheter et à installer de tels systèmes, mais quelles sont les considérations et les barrières non techniques à étudier pour que l'on puisse s'acheminer vers un bureau automatisé ("sans papier") ?

2.0 LOIS SUR L'INFORMATION

2.1 Définitions

L'information ou les données jouent un rôle de plus en plus important dans la société et dans l'économie, en général, et dans les différentes organisations, en particulier. Il ne faut donc pas s'étonner de la rapide augmentation du nombre des lois, règlements, codes, lignes directrices, règles, etc., aussi bien nationaux qu'internationaux, qui régissent ce que l'on peut, ne peut pas ou encore devrait faire, pour ce qui a trait à l'information enregistrée. En même temps, les lois ou principes juridiques en place qui nous inspiraient jusque-là une grande quiétude semblent tout à coup ne plus convenir ni s'appliquer à l'univers numérisé de l'électronique. Ceux qui comptaient sur ces lois pour assurer une certaine garantie de rendement de l'investissement se trouvent soudainement sans recours à la loi.

Ce problème est généralisé. Il est maintenant rare qu'on adopte ou révise un statut ou un règlement sans tenir compte de son applicabilité à tel ou tel aspect de l'univers numérisé et électronique. Le présent document expose la notion de loi sur l'information pour couvrir toute loi et tous règlements qui en découlent, ou parties de ces lois ou règlements, qui traitent de l'information enregistrée d'une façon ou d'une autre.

Les présentes définitions que la loi donne de "document", "produire", "conserver" et "maintenir" sont propres à une technologie (soit celle du papier). Des définitions nouvelles, plus génériques et plus indépendantes de la technologie, sont nécessaires. Les sections qui suivent proposent trois définitions de base, soit celles de :

- "information enregistrée",
- "manipulation de l'information",
- "loi sur l'information".

2.1.1 Information enregistrée

Il serait utile de noter que les termes "données", "information", "document", etc. sont employés indifféremment dans ce document. Ils désignent tous l'"information enregistrée". Voici la définition de l'"information enregistrée" :

> "information ou données enregistrées, indépendamment de leur support physique, appartenant à une organisation (propriété) ou dont l'accès, l'utilisation ou l'élimination sont régis par une organisation et/ou qui peuvent aisément être compilées ou extraites des systèmes informatiques sous de nouvelles formes ou combinaisons, à l'aide des outils et des mécanismes disponibles dans le cours habituel et ordinaire des activités".

Si les systèmes informatiques intégrés, et surtout les systèmes bureautiques intégrés, doivent un jour ou l'autre devenir le soutien essentiel de toutes nos activités, soit dans un "univers automatisé", il faudra réviser ou modifier la définition de "document", etc. dans toutes les lois et tous les règlements, en le remplaçant par un terme générique et indépendant de la technologie, soit "information enregistrée".

2.1.2 Manipulation de l'information

Ce document présente, de même, le principe de la manipulation de l'information, ce terme étant employé à titre générique, pour couvrir les nombreux genres de fonctions ou d'activités qui peuvent s'exercer à l'égard de l'information enregistrée, notamment :

> "toute fonction concernant l'information enregistrée, telle que la création ou la collecte, le traitement, le stockage, l'extraction, la communication ou la circulation, la diffusion et la distribution, l'accès et l'utilisation, la protection (sécurité, protection des renseignements confidentiels ou personnels, etc.), la conservation, l'élimination, l'archivage, etc."

"Manipulation de l'information" est donc le terme générique employé pour désigner toute la gamme des moyens d'enregistrement et de stockage et toutes les fonctions pouvant être exécutées à l'aide des technologies de l'informatique et des télécommunications. Il s'agit là également d'un terme qui n'est pas automatiquement associé à une technologie particulière.

2.1.3 Lois sur l'information

Le niveau de préoccupation et le degré d'informatisation ont atteint un plateau, où il est devenu utile de regrouper un ensemble de lois et de règlements sous la catégorie "lois sur l'information"[1]. On peut définir ainsi l'expression "loi sur l'information" :

> "loi, règlement, politique ou code (en tout ou en partie) qui exige la création, la production, l'extraction, la présentation, la conservation, le stockage ou la destruction d'informations enregistrées, ou encore qui pose des conditions à l'accès, à l'utilisation, à la confidentialité, à la reproduction, à la diffusion, à la transmission, à la vente, au partage ou à la manipulation d'informations enregistrées".

Au fond, les lois sur l'information et les exigences connexes peuvent être réparties en un certain nombre de catégories, selon qu'elles:

- exigent que l'on conserve ou retienne certaines données pour des périodes déterminées, auquel cas, on parle couramment d'exigences de conservation des documents;

- exigent que l'on puisse produire ou extraire des données (par exemple pour les inspecteurs, dans certaines industries);

- exigent que l'on présente des données à un gouvernement ou un organisme de réglementation (par exemple données sur l'impôt, données sur les douanes, présentation aux commissions de réglementation de l'échange de valeurs);

- exigent que l'on crée des données si l'on entreprend une activité particulière (par exemple données sur l'exposition aux radiations, données sur les émissions);

- exigent que l'on détruise des données (par exemple documents classifiés ou renseignements sur des personnes);

- exigent que l'on protège des données (par exemple données sur la vie privée, renseignements rassemblés en vertu de la Loi sur la statistique ou de la Loi de l'impôt sur le revenu);

- posent des conditions à l'accès, l'utilisation ou la confidentialité de l'information enregistrée (par exemple accès à l'information ou aux secrets officiels, nouveaux articles du Code criminel sur la fraude informatique et sur l'abus des données, confidences d'un client à son avocat, etc.);

- posent des conditions sur la façon de traiter l'information (par exemple Loi sur la preuve, règlements et normes financiers, etc.);

- posent des conditions sur la production, la distribution ou la vente d'informations enregistrées (par exemple droits d'auteur, marques de commerce, écrits haineux, pornographie);

- posent des conditions sur le partage, le chaînage ou la circulation de l'information (par exemple protection des renseignements personnels, restriction du transfert technologique); et

- posent des conditions pour l'emplacement où les données sont manipulées (par exemple Loi sur les banques ou "au siège social").

La plupart des lois sur l'information sont émises aux niveaux national et provincial. Cependant, la législation internationale dans ce domaine augmente. À noter qu'à ce dernier niveau, l'évolution de la législation résulte en bonne partie de la coopération des gouvernements et des entrepri-

ses pour l'élaboration de normes et de codes, mutuellement acceptables, le plus souvent à titre volontaire.

À noter aussi que les catégories de lois sur l'information décrites plus haut ne s'excluent pas nécessairement l'une l'autre. De fait, les lois touchant la manipulation de l'information enregistrée comportent souvent plusieurs de ces catégories à la fois. Il faut considérer les lois sur l'information dans la perspective beaucoup plus vaste présentée plus haut, et non les limiter à quelques catégories portant sur les droits d'auteur, les marques de commerce, les brevets, la télédiffusion ou la publication. On retrouve également des éléments de loi sur l'information dans les droits garantis par la Charte canadienne des droits et libertés, tels que la liberté d'expression, la liberté de la presse et des autres moyens de communication.

Les informaticiens de même que les décideurs d'une organisation ne doivent pas sous-estimer l'importance présente, qui ne cesse de croître, de la législation sur l'information. Que l'on gère ou utilise des systèmes informatiques gros ou petits, que l'on élabore des applications ou conçoive des systèmes, etc., il faut connaître les exigences des lois sur l'information applicables à l'organisation que l'on sert ainsi qu'aux données traitées au moyen de ces systèmes. Peu importe la technologie utilisée pour manipuler l'information enregistrée dans l'organisation dont on relève, on doit toujours soit se conformer aux exigences de telles lois, si elles sont obligatoires, soit en tenir compte, si elles ne le sont pas.

2.2 Récents changements dans la législation canadienne sur l'information

Il est vrai que de nombreuses lois sur l'information sont particulières à une activité ou à une industrie, mais il existe un certain nombre de lois importantes sur l'information dont toutes les organisations doivent tenir compte. Ce sont la Loi sur la preuve au Canada, les nouveaux articles, récemment adoptés, du Code criminel au sujet de la fraude informatique et de l'abus des données, de la conservation des documents et des droits d'auteur et, de plus en plus, dans le secteur public et, à un certain degré, dans le

secteur privé également, la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels.

Les exemples qui suivent sont basés sur le contexte canadien, mais il existe des problèmes ou des défis semblables, en ce qui concerne les lois sur l'information, dans la plupart des pays.

2.2.1 Code criminel

En février 1983, la Société canadienne de l'informatique a organisé, avec l'aide du ministère fédéral de la Justice, une "Consultation nationale sur les modifications du Code criminel portant sur les abus informatiques". Des représentants d'organisations très diverses et des experts particuliers y ont participé. L'objet de cette consultation était de discuter en vue de trouver des moyens de modifier le Code criminel pour couvrir les actes couramment désignés par "fraude informatique" et "abus de données" et pour en informer le ministère de la Justice. D'après les résultats des conflits portés alors devant les tribunaux, il était manifeste que les dispositions du Code criminel relatives au vol d'un service de télécommunications, comme l'indique l'article 287(1) du Code criminel, ne pourraient s'appliquer à des notions telles que "le vol de temps d'ordinateur ou d'un service informatique", ou encore "le vol ou le détournement de données".

Cette constatation a semé l'inquiétude dans les associations industrielles et professionnelles. L'utilisation des technologies reliées à l'ordinateur avait atteint, dans de nombreux secteurs industriels et entreprises privées, le stade où non seulement ceux-ci avaient consacré des ressources considérables à la construction de systèmes informatiques de stockage des documents, mais étaient devenus très tributaires de ces systèmes, qui représentaient alors un instrument de soutien indispensable pour les opérations journalières. Une vague d'inquiétude envahissait les organisations : à mesure que celles-ci tiraient parti des nouvelles technologies informatiques pour rendre leurs opérations plus efficaces et plus rentables, allaient-elles se retrouver soudain sans recours à la protection de la loi, pour la seule

raison qu'au lieu d'enregistrer leurs informations sur papier, elles le faisaient sous forme électronique ?

La "consultation" de deux journées visait des secteurs très divers, reliés aux répercussions technologiques sur la loi et les principes juridiques (par exemple les données sont-elles un bien, une propriété ?). Voici, en résumé, les résultats de la consultation :

- le détournement ou la destruction d'informations appartenant à quelqu'un, qu'il s'agisse d'un programme informatique ou d'un document assimilable par la machine, doit être considéré comme une fraude, indépendamment du support sur lequel ces informations sont enregistrées ou de la forme qu'elles revêtent;

- étant donné les caractéristiques exclusives et nouvelles du système informatique et des données informatiques ou électroniques, le Code criminel doit être modifié pour traiter expressément de ces questions;

- il faut prévoir, pour la "fraude informatique", un article distinct, pareil à celui qui traite de la fraude en télécommunications; et

- l'on doit ajouter un article qui traite expressément du problème de l'"abus des données", lequel ne doit pas être confondu avec les droits de propriété intellectuelle (par exemple droit d'auteur).

Un an plus tard, soit le 7 février 1984, un projet de loi omnibus visant à modifier le Code criminel, le projet C-19, était déposé, mais il est demeuré sans lendemain. Réintroduit plus tard sous le nom de projet de loi C-18, il contenait des modifications précises portant sur la fraude informatique et sur l'abus des données. Ces modifications ont été adoptées le 24 avril 1985, sous réserve de quelques changements par la Chambre des Communes et ont reçu la sanction royale, c'est-à-dire qu'elles sont entrées en vigueur le 5 décembre 1985. Deux nouveaux articles présentent un intérêt particulier, soit :

- l'article 301.2, qui traite de l'usage non autorisé de l'ordinateur;

et

- l'article 387.1(1.1), qui instaure la notion de méfait pour ce qui a trait aux données.

Le projet de loi C-18 a également donné de nouvelles définitions de "programme d'ordinateur", "service d'ordinateur", "ordinateur", "données", "fonction", "intercepter" et "dispositif électromagnétique, acoustique, mécanique ou autre".

Voici le libellé de l'article qui traite de l'usage non autorisé d'un ordinateur :

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

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

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

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

est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable par procédure sommaire."

Ce nouvel article sur la fraude informatique non seulement introduit dans la loi la notion de vol d'un service informatique (ou d'ordinateur), comme la notion qui existe déjà pour les services de télécommunications, en vertu de l'article 287(1), mais rend également illégal tout genre d'espionnage élec-

tronique, d'interruption d'une opération d'ordinateur ainsi que la programmation d'un ordinateur pour tenter systématiquement d'établir un accès non autorisé à un système informatique. Cette dernière technique a la faveur du "pirate" de l'ordinateur. Du point de vue de la mise en vigueur de la loi, il semble y avoir peu ou pas de différence entre un appareil de télécommunications et un ordinateur, en ce qui concerne l'usage illégal. Étant donné qu'il devient de plus en plus difficile, dans bien des cas, de distinguer un ordinateur ayant des fonctions de télécommunications d'un appareil de télécommunications ayant des fonctions informatiques, cette clause est très utile et rend la présente loi canadienne bien plus simple à administrer que les lois en vigueur aux États-Unis ou en Europe.

Deuxièmement, voici le libellé du nouvel article sur l'abus des données :

"a.386.1 Commet un méfait quiconque, volontairement,

a) détruit ou modifie des données;

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

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

Il convient d'ajouter plusieurs remarques au sujet de l'article sur l'abus des données :

1) la formulation est à la fois précise et suffisamment compréhensive pour couvrir toute intervention possible sur les données, y compris la suppression de données;

2) du point de vue de la mise en vigueur de la loi, le mot clé ici est "volontairement". En d'autres termes, il semble qu'il faut prévoir, dans son système et dans ses procédures d'exploitation ainsi que dans les instructions, des caractéristiques qui empêchent les données d'être modifiées ou supprimées "accidentellement";

3) même si cet article ne précise pas que l'addition de données (c'est-à-dire l'addition de fausses données) est une fraude, on peut soutenir qu'une telle intervention gênerait "l'emploi légitime des données" et inclurait la "modification" d'ensembles de données, de même que l'usage non autorisé d'une fonction d'ordinateur, s'il y a lieu;

4) puisqu'un programme ou logiciel d'ordinateur consiste, par définition, presque entièrement en données, ce nouvel article doit également couvrir n'importe quel "vol" de programmes d'ordinateur appartenant à quelqu'un, puisqu'un tel "vol" comporterait forcément un acte "volontaire" et "non autorisé" commis sur l'ordinateur et sur les données.

Voici quelques nouvelles définitions, que donne l'article 301.2(2) :

"programme d'ordinateur" : un ensemble de données qui représentent des instructions ou des relevés et qui, lorsque traités par l'ordinateur, lui font remplir une fonction;

"service d'ordinateur" : s'entend notamment du traitement des données de même que de la mémorisation et du recouvrement ou du relevé des données;

"ordinateur" : un dispositif ou un ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs :

a) contiennent des programmes d'ordinateur ou d'autres données;

b) conformément à des programmes d'ordinateur :

(i) exécutent des fonctions logiques et de commande, ou
(ii) peuvent exécuter toute autre fonction;

"données" : représentations d'informations ou de concepts qui sont préparés ou l'ont été de façon à pouvoir être utilisés dans un ordinateur;

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

"fonction" : s'entend notamment des fonctions logiques, arithmétiques, des fonctions de commande et de suppression, des fonctions de mémorisation et de recouvrement ou de relevé des données de même que des fonctions de communication ou de télécommunication de données à destination, à partir d'un ordinateur ou à l'intérieur de celui-ci.

"intercepter" : s'entend notamment du fait d'écouter ou d'enregistrer une fonction d'un ordinateur ou de prendre connaissance de sa substance, de son sens ou de son objet.

Ces modifications présentent un intérêt particulier, en ce qu'elles peuvent offrir beaucoup de possibilités dans le traitement du problème de la reproduction "illégale" de logiciel. On pourrait expliquer ces possibilités de plusieurs façons.

On pourrait, par exemple, arguer qu'une telle reproduction comporte le lancement d'une fonction d'ordinateur sans aucune apparence de droit ou qu'elle pourrait être considérée comme un emploi illégal de données, puisque la définition de données inclut des instructions. La question des droits d'auteur est traitée en détail plus loin, mais on peut faire valoir ici que l'emploi "créatif" de ces modifications du Code criminel pourrait aider à enrayer l'usage, vastement répandu, de la reproduction "illégale" de programmes. Le cas s'est présenté récemment : la Loi sur les marques de commerce avait été invoquée avec succès pour poursuivre quelqu'un qui avait, en fait, violé les droits d'auteur relatifs à un logiciel.

À noter, par ailleurs, que la modification relative à l'abus des données élude la question de considérer ou non les données comme un avoir, en ajoutant l'article 387(4) qui prévoit des sanctions pour les méfaits portant sur les données, indépendamment des clauses prévues pour la propriété en général. En outre, elle n'attribue pas aux méfaits relatifs aux données la valeur minimale de 1 000 $ prévue pour les méfaits contre la propriété.

Pour une fraude informatique, la peine prévue peut aller d'une déclaration sommaire de culpabilité à dix années d'emprisonnement, alors que pour les méfaits relatifs aux données, elle va de la déclaration sommaire de culpabilité à deux années d'emprisonnement.

Enfin, il serait utile d'attirer l'attention des informaticiens et gestionnaires de l'information sur un nouvel article 387(5.1) qui se lit comme suit :

> "Est coupable :
>
> a) soit d'un acte criminel et passible d'un emprisonnement maximal de cinq ans,
>
> b) soit d'une infraction punissable par procédure sommaire,
>
> quiconque volontairement accomplit un acte ou volontairement omet d'accomplir un acte qu'il a le devoir d'accomplir, si cet acte ou cette omission est susceptible de constituer un méfait qui cause un danger réel pour la vie des gens ou de constituer un méfait à l'égard de biens ou de données."

Selon cette clause, il semble que les gestionnaires du système informatique sont tenus d'agir en "<u>bons régisseurs</u>" et de veiller à ce que des dispositions de sécurité et de protection des renseignements confidentiels sont en place pour leurs systèmes et les données que ceux-ci contiennent. Prenons, par exemple, le cas de gestionnaires de systèmes informatiques de soutien des fonctions vitales d'un hôpital - telles que la surveillance et la com-

mande de systèmes de maintien de la vie : si ces gestionnaires n'instaurent pas de mesures de sécurité qui protègent adéquatement de telles opérations contre l'accès non autorisé et l'ingérence possible, soit de pirates ou d'employés mécontents, ils s'exposent au risque d'être accusés en vertu du Code criminel.

À ce sujet, l'auteur trouve fâcheux que les gestionnaires de systèmes informatiques soient rarement renvoyés lorsque des "pirates" accèdent à ces systèmes ou les manipulent illégalement, d'autant plus que ces malfaiteurs doivent leur aptitude à y pénétrer surtout à leur persévérance ou à la chance et, en particulier, à l'absence de fonctions de sécurité de base dans de nombreux ordinateurs ou appareils de communication.

Dans ce contexte, le "Code d'éthique et des normes de la conduite professionnelle" [2] publié par la Société canadienne de l'informatique en janvier 1985 revêt encore plus d'importance. Cette Société ainsi que d'autres associations de personnes ou d'industries auraient intérêt à se demander sérieusement s'il est utile et approprié d'élaborer un code qui explique l'obligation qu'ont les informaticiens de bien régir les données (y compris les instructions du logiciel), en vertu de l'article 387(5.1).

2.2.2 Loi sur la preuve

Si, d'une part, les nouvelles modifications du Code criminel au sujet de la fraude informatique et de l'abus des données reconnaissent clairement l'importance et la valeur des systèmes et des données informatiques, en prévoyant la protection de ces ressources, d'autre part, une question de droit majeure reste encore à régler au sujet des systèmes informatiques intégrés. Il s'agit de l'admissibilité des documents créés par ordinateur à titre de preuve en cour. Il y a plus de dix ans que l'on reconnaît la nécessité de modifier la Loi sur la preuve au Canada, mais il a fallu attendre jusqu'au printemps de 1985 pour que des efforts concertés soient déployés afin de chercher à résoudre la question de la validité de la preuve informatisée. Le ministère de la Justice avait alors demandé à l'Association des administrateurs et des gestionnaires des documents (ARMA) d'organiser une consulta-

tion nationale axée sur la validité de la preuve informatisée (CNVPI) [3]. Des organisations professionnelles, industrielles, syndicales et autres, nombreuses et représentatives, ont participé à la CNVPI.

Dans l'un des documents établis aux fins de la CNVPI, on notait que "en l'absence de lignes directrices claires sur la validité des sorties d'ordinateur ainsi que des signatures et des autorisations produites électroniquement, de même que sur le poids qui leur est accordé, chaque organisation conserve des volumes considérables de documents de papier pour enregistrer les transactions et réduire les coûts de conflits éventuels. La conservation de ces copies sur papier d'informations déjà stockées sous forme informatique ajoute aux frais généraux et réduit la compétitivité" [4]. L'étude ajoutait que la paperasserie dans les bureaux augmentait au rythme de 20 % par année et que, pendant la durée d'un document, on en tire environ 19 copies. Ces copies sont presque toutes classées, mais on ne les consulte jamais par la suite. Le rapport de l'étude concluait que "l'adaptation des critères de validité aux systèmes informatiques de gestion de l'information que les entreprises utilisent, et souhaitent continuer à utiliser, accroîtra l'usage de la technologie. Il s'ensuivra de nouvelles économies d'échelle, un rendement supérieur de l'investissement dans les systèmes informatiques ainsi qu'un meilleur soutien à la décision et l'augmentation de la productivité. L'existence de critères officiels de validité garantira, de plus, la convergence des efforts sur la protection de l'intégrité des informations des organisations [...]. L'admissibilité, à titre de preuve, des documents créés par ordinateur présente d'autres avantages : les entreprises seront moins tributaires d'un système sur papier de soutien à la décision et, en conséquence, réduiront ou peut-être même élimineront les documents de papier".

Dans le même ordre d'idée, l'ARMA, dans son exposé à la CNVPI, déclarait que "pour la plupart des organisations, surtout les entreprises, la prédominance de l'usage de systèmes informatiques de conservation de l'information et des documents est indispensable à leur survie et à leur aptitude à réduire les coûts pour demeurer compétitifs dans leur domaine. Pour continuer à soutenir la concurrence nationale et internationale, les entreprises canadiennes

n'ont d'autre choix que d'adopter ou d'utiliser les technologies disponibles les plus rentables [...]. Les membres de l'ARMA s'inquiètent beaucoup de ce qu'ils ne peuvent pas tirer pleinement parti des nouvelles technologies pour fournir des services plus efficients et plus rentables à leurs organisations. En effet, s'ils utilisent ces technologies au maximum, ils risquent de nuire à leurs chances de sortir vainqueurs des conflits, soit à titre de défendeurs, soit à titre de plaignants"[5].

La cour ne peut agir que d'après la preuve soumise correctement. "La question de "validité" est donc primordiale aux fins de la Loi sur la preuve. Pour déterminer si une preuve est valide, le juge doit d'abord déterminer si elle est "pertinente" [...]. Une preuve non pertinente est, par conséquent, toujours inadmissible. Cependant, une preuve pertinente peut quand même être inadmissible parce qu'elle viole l'une des règles d'exclusion" [6]. Dans l'ensemble, les cours préfèrent recevoir une preuve d'un témoin ayant une connaissance directe des faits en question et être en mesure de contre-interroger le témoin. En d'autres termes, les cours ne reconnaissent pas l'ouï-dire. Toutefois, avec les siècles, des pratiques ont pris naissance, faisant exception à la règle de l'ouï-dire, telles que l'acceptation de documents gouvernementaux, bancaires, commerciaux et médicaux établis dans le "cours normal des affaires". Ces exceptions se justifient par la très faible probabilité que de tels documents soient erronés, puisque l'entreprise ou le gouvernement lui-même comptent sur ces documents pour prendre des décisions et effectuer leurs opérations.

Autre exclusion majeure de la règle de l'ouï-dire : la règle de la meilleure preuve. En substance, celle-ci exige que, s'il existe un original du document, celui-ci soit produit en cour. Cependant, avec les années, dans certaines circonstances, la cour admet des copies et des duplicatas (par exemple des documents bancaires).

À présent, la situation de l'admissibilité des documents créés par ordinateur n'est pas claire. Au Canada, la jurisprudence est très limitée et incohérente en la matière. À la Consultation nationale, c'est-à-dire la CNVPI, les questions majeures soulevées sont les suivantes :

- la pertinence de notions telles que "original", "duplicata" et "copie" en ce qui concerne les documents créés par ordinateur;

- l'explication de l'expression "dans le cours normal des affaires", lorsqu'on utilise de plus en plus des systèmes de soutien à la décision interactifs et en temps réel, où le "document" n'est généré qu'à la demande de l'utilisateur, souvent d'une façon exclusive et personnalisée;

- le rôle des normes de traitement des données et la détermination de la possibilité d'appliquer de telles normes;

- l'opportunité de l'application des mêmes règles d'admissibilité de documents créés par ordinateur à tous les documents, qu'ils soient émis par une banque, un gouvernement, une entreprise ou un établissement médical.

Dans le présent contexte, il faut noter que la situation des documents bancaires est particulière pour ce qui a trait à l'admissibilité. "On avance parfois qu'il faut appliquer une norme d'admissibilité moins stricte aux documents, manuels ou générés par ordinateur, des banques et des établissements financiers, puisque ceux-ci doivent balancer leurs livres tous les jours et qu'ils sont soumis continuellement à l'examen non seulement de leurs vérificateurs, mais également de leurs clients. Toutefois, le gouvernement et les entreprises non financières pourraient rétorquer que leurs dossiers sont aussi soigneusement tenus et soumis à la vérification [...]. De fait, certains organismes gouvernementaux et entreprises non financières peuvent être plus méticuleux dans la tenue de leurs dossiers que certains établissements financiers" [7].

Une nouvelle Loi uniforme sur la preuve, applicable aux niveaux fédéral et provincial, a été rédigée mais n'avait pas encore été déposée lors de la rédaction de ce rapport de recherche. Cependant, il est utile de noter les recommandations de la CNVPI. En résumé, celle-ci suggère que la Loi sur la

preuve au Canada soit modifiée comme suit pour prévoir l'admissibilité des documents créés par ordinateur :

- addition de nouvelles définitions concernant les ordinateurs et les documents produits par ordinateur, telles que celles des termes suivants :

  - "ordinateur" (comme dans le Code criminel);

  - "données" (comme dans le Code criminel); et

  - "original" (clause distincte visant les documents informatiques, chacun de ceux-ci étant considéré comme "original");

- addition de clauses au présent article sur l'authentification :

  - addition d'un paragraphe pour l'établissement de l'authenticité d'un document créé par ordinateur, au moyen de la déclaration verbale, ou par affidavit, d'un témoin;

  - addition d'un paragraphe qui prévoit l'authentification, au moyen d'affidavits, avec possibilité d'inclure des formules modèles, c'est-à-dire une pour l'utilisateur des données et une autre pour l'agent de traitement de celles-ci, s'il s'agit de deux personnes distinctes, dans les règlements qui font suite à une nouvelle Loi sur la preuve au Canada;

- pour ce qui a trait aux documents commerciaux d'établissements financiers, l'addition d'un paragraphe prévoyant l'acceptation d'un document commercial dans des poursuites lorsque l'établissement n'est pas partie, aux fins de la preuve, à moins qu'on ne prouve le contraire;

- l'application des mêmes règles à n'importe quel document créé par ordinateur, que ce document soit commercial, financier, médical ou gouvernemental.

Il a été également proposé que, pour garantir un niveau acceptable d'intégrité et de fiabilité aux données, l'organisation pourrait étendre la fonction de vérification interne et externe à la gestion de l'information aussi bien qu'à la gestion financière, selon la notion de "vérification intégrée". Les établissements qui pratiquent ce genre de vérification auront peu ou pas de difficultés à produire en cour, à titre de preuves, des extraits de base de données informatiques. De plus, il a été recommandé de prévoir deux genres d'affidavits : un pour la personne qui crée ou utilise les données en question, c'est-à-dire l'utilisateur des données, et l'autre pour le responsable du système informatique, c'est-à-dire l'agent de traitement des données [8]. Enfin, on a convenu qu'il était impossible d'établir une norme unique pour le traitement des données. Cependant, il est peut être possible ou utile d'élaborer des normes pour des applications précises et bien définies ayant leurs propres pistes de vérification et de transactions documentables. En somme, le secteur le plus prometteur des normes relatives aux données est manifestement celui des unités de sortie, surtout celles qui sont destinées au stockage permanent des données, c'est-à-dire le disque optique qu'on peut mettre à jour, mais non effacer. À ce propos, il convient de signaler l'élaboration et l'approbation, en 1979, d'une norme de traitement pour la technologie des microfilms. Intitulée "Microfilm preuve littérale/Microform as Documentary Evidence", c'est une norme nationale canadienne (CAN2-72.11-79), approuvée par le Conseil canadien des normes.

2.2.3 Loi sur l'accès à l'information et Loi sur la protection des renseignements personnels

Le Code criminel et la Loi sur la preuve sont tous deux des exemples de lois d'applicabilité générale, touchant tous les types de systèmes informatiques. Il existe également des lois particulièrs sur l'information qui stipulent de nouvelles exigences juridiques pour l'information enregistrée et la manipulation de l'information. Ces lois tendent à se dissocier de la technologie

dans leur application. À présent, la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels au Canada ne s'appliquent qu'à des établissements publics précis du secteur fédéral et dans certaines provinces. Toutefois, le Canada s'est engagé à encourager le secteur privé à adhérer volontairement aux "Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel" de l'OCDE.

Jusqu'à présent, les informaticiens considéraient souvent les lois sur la protection des renseignements personnels comme une intrusion injustifiée, un élément négatif, dans les systèmes informatiques, ce qui est une erreur. En substance, ces lois exigent la tenue de renseignements personnels opportuns, exacts et pertinents uniquement. Elles stipulent qu'il ne soit pas fait un mauvais usage de cette information et que celle-ci soit recueillie à des fins précises ou définies, et ce, directement auprès des intéressés, à qui l'on doit donner ensuite l'occasion de voir cette information et de demander des corrections ou des suppressions, s'il y a lieu.

Les lois sur la liberté de l'information, en donnant des droits d'accès, déterminent en même temps les catégories particulières d'informations confidentielles (ou précieuses), qu'il faut protéger contre toute divulgation non autorisée. Les deux genres de lois présentent le principe de l'imputabilité publique des gestionnaires de l'information, en exigeant d'eux la production d'index annuels et l'aptitude à reconnaître et à extraire rapidement des informations déterminées. Ainsi, les deux genres de lois favorisent de bonnes méthodes relatives à l'information.

2.2.4 Exigences en matière de conservation des documents

Selon une analyse de toutes les exigences fédérales relatives à la conservation des documents dans les entreprises au Canada, en 1982, des 76 lois et 111 règlements en vigueur alors, la plupart ne permettaient pas la conservation de telles informations sous forme assimilable par la machine. La cause en est que la définition de "document" vise encore les documents sur papier. Avant de concevoir des systèmes informatiques intégrés pour remplacer les

opérations sur papier, surtout celles des bureaux, les informaticiens feraient bien d'examiner les aspects juridiques des exigences de conservation des documents.

2.2.5 Droit d'auteur

Dans les Lois sur l'information, il existe une partie qui a suscité des débats considérables, c'est la question du droit d'auteur appliqué au logiciel et, de plus en plus, aux bases de données. Ces débats se sont ressentis de l'échec des tentatives visant une nette distinction entre l'abus des données, c'est-à-dire le vol de données, y compris d'ensembles d'instructions, et les failles de la législation sur le droit d'auteur. La nécessité de protéger les ressources en informations enregistrées (données ou logiciel) de l'entreprise contre l'accès non autorisé ou le vol, c'est-à-dire l'abus des données, ne doivent pas être confondues avec le désir d'obtenir un rendement convenable de l'investissement (concret ou intellectuel). Les droits d'auteur touchent essentiellement le contrôle de la distribution de l'information enregistrée, sous quelque forme qu'elle se présente, qui, le plus souvent, est déjà une information publique. Il s'agit là de l'inverse de la préoccupation des gestionnaires de l'information qui désirent protéger les biens ou les ressources de leur organisation, sous forme d'informations enregistrées, contre la divulgation non autorisée (par exemple par copie) et que la distribution ou la vente de ces ressources n'intéressent pas du tout.

Pour ce qui a trait au droit d'auteur, il serait donc utile d'établir la distinction entre, d'une part, les logiciels et les données appartenant à une organisation qui les considère comme faisant partie de ses avoirs (ou de ses "biens") et qui ne compte jamais les distribuer et, d'autre part, les logiciels (ou données) destinés à la distribution et à la vente. Le premier cas pourrait être couvert par les nouvelles dispositions du Code criminel. Du point de vue économique, la Loi sur le droit d'auteur est un mécanisme utilisé pour garantir un rendement équitable du capital de ceux qui ont investi des ressources pour pouvoir distribuer et vendre à d'autres quelque chose ayant une certaine valeur. Dans ce contexte, le Code criminel proté-

gera les "biens", sous forme de "données" et de "logiciel", contre leur détournement de leur propriétaire, qui ne cherche pas à les distribuer ou à les vendre, c'est-à-dire ne désire pas les rendre "publics". À ce propos, les données et le logiciel en question peuvent très bien représenter la "substance" de l'entreprise et donner à celle-ci l'avantage sur la concurrence (par exemple : services financiers).

Un éditeur de "données" ou de "logiciels" est, par définition, quelqu'un qui désire distribuer ces produits, mais qui a besoin d'une garantie de rendement de son investissement. Pour cette raison, l'élaboration d'une législation nouvelle sur le droit d'auteur doit tenir compte des mesures correctives qui existent déjà en vertu des nouveaux articles du Code criminel sur la fraude informatique et l'abus des données.

3.0 CONSIDÉRATIONS PRATIQUES

Après avoir présenté et expliqué la notion de loi sur l'information ainsi que sa portée sur les systèmes informatiques intégrés, et après avoir exposé certaines questions de droit importantes et les récents développements dans les lois sur l'information au Canada, ce document passe à sa troisième et dernière section, pour faire état de quelques considérations pratiques et des questions de droit non encore résolues. Or cette résolution est considérée comme une condition préalable nécessaire pour l'informatisation intégrale du lieu de travail.

3.1 Définition de "document" : de l'objet à l'information

En droit, la définition classique d'"information enregistrée" est celle d'un document, celui-ci étant généralement défini comme un objet ou une pièce physique sur lequel l'information est inscrite; et, lorsqu'il existe une relation biunivoque entre l'information enregistrée et le support de celle-ci, qui n'est pas réutilisable, est fixé dans le temps, dans l'espace et dans la forme et est basé sur des notions telles que "original", "duplicata" et "copie".

Le principal impact des nouvelles technologies informatiques sur les lois régissant l'information est le déplacement de l'importance accordée à la pièce physique, ou support de l'information, vers l'information ou les données elles-mêmes, c'est-à-dire du document à l'information enregistrée. Du point de vue de la manipulation de l'information, cet impact représente le passage de la gestion d'objets physiques ou documents à celle de l'information ou des données, aucune relation biunivoque n'existant plus entre le support de stockage et l'information stockée et ce support étant même réutilisable. La nouvelle législation, telle que les modifications du Code criminel, les modifications proposées pour la Loi relative aux enquêtes sur les coalitions, la Loi sur les faillites, les lois fédérales et provinciales de l'accès à l'information et de la protection des renseignements personnels, contient partout des définitions de "document", "renseignement",

"information" ou "données" qui ne sont pas particulières à une technologie déterminée. En même temps, un nombre considérable de lois continuent d'exister, alors que leur définition de "document" est périmée ou inappropriée du point de vue de la nouvelle technologie informatique. En conséquence, si l'on passe d'un système basé sur le papier à un système informatique intégré, on peut découvrir qu'une loi particulière ne s'applique plus ou qu'il y a confusion quant au mode d'application d'une loi ou quant aux lois qui s'appliquent. Il peut très bien arriver que l'interprétation stricte d'une loi ou d'un règlement empêche quelqu'un d'instaurer des technologies informatiques nouvelles, plus efficientes ou rentables. Il en est ainsi surtout pour les exigences présentes sur la conservation des documents.

L'une des considérations pratiques à l'usage de ceux qui ont des intérêts dans les secteurs de la technologie informatique consiste à plaider pour la modification des lois sur l'information en vigueur, à n'importe quel niveau de juridiction, pour que la définition de "document", "information enregistrée" ou "données" devienne indépendante de la technologie et soit uniforme. La définition de base pourrait simplement être "information enregistrée". Si une définition uniforme d'"information enregistrée" n'est pas possible, il faut s'assurer que les variantes de la définition sont, au moins, compatibles les unes avec les autres. Cette question revêt une importance particulière lorsqu'on intègre plusieurs systèmes informatiques qui sont actuellement exploités en tant qu'applications distinctes. Il se peut facilement, en conséquence, que plusieurs lois sur l'information s'appliquent en même temps à de tels systèmes informatiques intégrés.

Les lois sur l'information doivent également permetre le passage d'un support d'information à un autre et d'une technologie de manipulation de l'information à une autre, les lois sur l'information demeurant uniformément applicables. (La présente Loi sur les banques contient une telle clause.)

Cependant, pour ce qui est des articles d'application d'une loi, d'un règlement ou d'un code sur l'information, il est peut-être plus approprié et plus efficace de créer un paragraphe spécial pour traiter des aspects de

l'"information enregistrée" et de la "manipulation de l'information" particuliers à un type déterminé de technologie informatique. Les récentes modifications du Code criminel portant sur l'"abus des données" représentent un exemple approprié de cette approche.

3.2 Protection de l'information enregistrée

L'utilisation accrue des technologies informatiques s'accompagne d'une plus grande reconnaissance de l'information ou des données en tant que bien de valeur ou ressource. Cette reconnaissance et l'acceptation de l'information comme une ressource de valeur se reflètent par l'utilisation de plus en plus répandue, aussi bien dans le secteur public que dans le secteur privé, de notions telles que "gestion des ressources en informations", "gestionnaire de ressources en informations" ou "centre serveur".

De même, les modifications du Code criminel portant sur la fraude informatique et sur l'abus des données ont été déposées et adoptées grâce à un grand concensus du secteur privé, du gouvernement et des particuliers, soit que l'information ou les données sont une ressource précieuse qui exige le même niveau de protection, en vertu de la loi, que les biens.

Voici une considération (très) pratique pour les informaticiens responsables des systèmes informatiques : ils auraient intérêt à élaborer une déclaration ou un ensemble de règles qui définissent en quoi consiste un acte autorisé ou un acte non autorisé pour ce qui a trait aux données (et au logiciel) et à l'usage de leurs systèmes informatiques. Même s'il peut s'agir là d'une tâche relativement sans importance pour les applications autonomes, on ne peut pas en dire autant de la création d'un tel code sur l'accès et sur l'utilisation des systèmes informatiques intégrés, qui prend même davantage l'allure d'un défi dans le nouveau secteur des systèmes bureautiques intégrés.

Il importe, pour une organisation et pour les informaticiens, d'élaborer un tel code d'accès et d'utilisation, en prévoyant des niveaux appropriés de protection de la sécurité des systèmes informatiques intégrés (ou de toute

application informatique). En effet, si une organisation découvre qu'elle est victime d'une fraude informatique ou d'un abus de données présumé et désire se donner toutes les chances de succès dans ses poursuites, elle doit être en mesure de démontrer que l'activité en question avait été clairement non autorisée. Le gestionnaire de l'information doit donc s'assurer que chaque employé de son organisation ayant accès à un système ou à des données informatiques, de même que chaque utilisateur, sait exactement quelles utilisations des systèmes et des données informatiques sont autorisées et lesquelles ne le sont pas. Dans le même ordre d'idées, les responsables des systèmes informatiques actuels doivent veiller à ce que ceux-ci soient dotés de fonctions de sécurité suffisantes pour qu'il y ait certitude absolue que la fraude informatique ou l'abus de données n'était pas "accidentel".

3.3 Intégrité des données

Une des principales raisons pour lesquelles de nombreuses organisations hésitent à se convertir totalement aux systèmes informatiques intégrés ou au bureau informatisé est que les lois les plus importantes sur l'information, telles que la Loi sur la preuve, n'ont pas été modifiées pour prévoir l'admissibilité des documents créés par ordinateur à titre de preuve. Les nombreuses exigences sur la conservation des documents n'ont pas été modifiées, non plus, pour permettre aux entreprises de conserver ces documents sous forme électronique.

Les débats qui ont eu lieu à la CNVPI indiquaient très clairement, toutefois, que si l'on modifiait la Loi sur la preuve au Canada pour prévoir l'admissibilité de documents créés par ordinateur, les informaticiens devraient, en conséquence, être en mesure de démontrer la fiabilité et l'intégrité des données de leurs systèmes. Les questions sur l'intégrité des données et la fiabilité des systèmes ont d'ailleurs dominé les débats de la CNVPI. Aussi, l'un des principaux défis posés aux informaticiens, ainsi qu'à l'industrie et aux utilisateurs de la technologie informatique, est-il l'établissement de normes ou de méthodes, au moyen desquelles on puisse démontrer adéquatement l'intégrité des données et la fiabilité des systèmes pour favoriser l'admissibilité des documents créés par de tels systèmes.

Dans ce contexte, l'inclusion, dans les rôles et responsabilités des vérificateurs internes et externes, de la vérification du respect des lois sur l'information pourrait représenter une solution praticable et viable. Cette vérification porterait sur la fiabilité et la précision des données du système, sur les mesures de sécurité, etc. et constituerait un élément logique de la nouvelle tendance vers les "vérifications intégrées".

Parmi les principales questions de droit à résoudre figure le rôle des signatures et de l'authentification dans les systèmes informatiques intégrés. À ce jour, un bon nombre des systèmes importants qui exigent de telles fonctions sont des systèmes de traitement des transactions. Dans ce secteur, diverses vérifications et étapes de contrôle de validation ont été mises au point à un niveau de détail et de rigueur d'application qui suffit à assurer à la fois l'intégrité des données et l'authentification (par exemple : l'utilisation d'un guichet automatique, où l'emploi d'une carte à bande magnétique et l'introduction du code d'identification personnel de l'utilisateur, conjugués avec les applications contractuelles, font efficacement fonction de signature électronique).

L'un des grands défis, qui représente en même temps une question de droit, consiste dans la vérification des signatures électroniques pour les systèmes informatiques orientés vers le "document". Parmi les obstacles majeurs à l'avènement du bureau informatique figure la nécessité de signatures qui, avec d'autres éléments d'information, servent de preuve d'acceptation ou d'autorisation de tels documents ou de mesures déterminées. Même si l'on résolvait la question de la preuve, on demeure pris avec le problème de la vérification de la signature [9]. Les récents progrès réalisés en cryptographie et en systèmes d'identification personnelle (par exemple : empreintes digitales, reconnaissance de la rétine ou de la voix, identificateurs personnels, cartes à bande magnétique ou à hologrammes) ont rendu maintenant techniquement possible et faisable, conjointement avec le timbre horodateur, d'établir l'authenticité d'un "document électronique" qui n'est pas sur support de papier. Il faut plus de recherches et de travail pour déterminer comment mettre en oeuvre ces techniques, sur le plan opérationnel, et quels changements apporter aux lois sur l'information pour en faire une réalité,

surtout dans les systèmes "ouverts" (par opposition aux systèmes "fermés", tels que les SWIFT ou ceux qui comportent l'utilisation de guichets automatiques). La question est encore plus urgente à cause de l'essor récent de l'échange électronique de données (c'est-à-dire de l'échange électronique de documentation (soit sans papier entre les entreprises, aux fins des achats, des factures, des connaissements, des remises, etc.

3.4 Stockage des données et des documents électroniques

Dernière considération pratique : la question du stockage "permanent" des données, aux fins de la preuve et d'autres exigences juridiques, opérationnelles et d'archives. Pour les besoins de la preuve et d'autres raisons juridiques, les organismes du secteur privé, comme ceux du secteur public, conservent d'énormes volumes de documents sur papier, ce qui représente des dépenses considérables. Les technologies du microfilm peuvent réaliser jusqu'à 98 % d'économie en espace d'entreposage de l'information enregistrée et, si on les applique conformément à la norme de microfilmage précitée, les documents correspondants seront admissibles à titre de preuve. Cependant, le microfilm, en tant que support de stockage permanent, présente quelques inconvénients de base. Premièrement, il ne permet pas la consultation et l'extraction interactives des données. Deuxièmement, il n'est pas facile de réutiliser les données sur microfilm sans avoir à les réintroduire dans les systèmes informatiques, à l'aide d'opérations spéciales et, en plus, à reconstituer la structure de la base de données.

L'une des technologies prometteuses pour le stockage permanent des données est celle du disque optique, dont l'immense capacité de stockage semble s'accroître presque de jour en jour, à mesure que de nouvelles technologies sont mises au point. La technologie du disque optique qu'on peut mettre à jour, mais non effacer, jumelée avec les techniques appropriées d'authentification et d'enregistrement des transactions, semble être la solution pour le stockage (et l'extraction, s'il y a lieu) des dizaines de milliers de "documents" informatiques des systèmes bureautiques intégrés (par exemple : documents WORM).

Cependant, ici, comme dans d'autres secteurs d'application de la technologie informatique, d'autres questions de droit restent à régler (par exemple : le besoin d'une nouvelle Loi sur la preuve).

4.0 CONCLUSIONS

Il existe maintenant des solutions technologiques et de gestion qui permettent de s'acheminer vers les systèmes informatiques intégrés et le bureau automatisé. L'un des principaux obstacles à surmonter est la nécessité de modifier les lois locales, nationales et internationales sur l'information qui entravent actuellement le progrès vers un univers sans papier, tout en maintenant l'esprit et l'objet de ces lois.

Au plan individuel, les informaticiens feraient bien de se mettre au courant des exigences des lois sur l'information et d'évaluer l'impact de ces lois sur les systèmes informatiques. Ceux qui omettent de tenir compte de ces exigences dans la conception et l'exploitation de systèmes informatiques intégrés le font à leurs propres risques. Non seulement leurs organisations et eux-mêmes risquent d'être confrontés à de coûteux rattrapages, mais leurs infractions aux exigences des lois sur l'information peuvent entraîner la perte de droits et de fonds ainsi que des conséquences fâcheuses de conflits, ou même de peines et d'amendes en vertu du Code criminel.

Pour terminer sur une note plus positive, si l'on examine de près les exigences fonctionnelles découlant des lois sur l'information, pour ce qui a trait aux systèmes informatiques intégrés, on découvre qu'elles correspondent, en somme, aux bonnes méthodes de gestion de l'information. On peut même avancer que l'observation de ces lois encouragera l'élaboration de systèmes informatiques efficients et rentables. Mais il s'agit là d'une tout autre question.

NOTES BIBLIOGRAPHIQUES

1. Article antérieur traitant de la notion de "Loi sur l'information" : "Information law and information management", de Knoppers, Jake V. Th. Information Management Review, vol. 1, n° 3 (Hiver 1986), pp. 63-73.

2. Société canadienne de l'informatique, Code de l'éthique et des normes de la conduite professionnelle, Société canadienne de l'informatique, Toronto, janvier 1985, 9 p.

3. Association des administrateurs et gestionnaires de documents, Inc. (ARMA), Actes et communications de la Consultation nationale sur la validité de la preuve informatisée (CNVPI), 28 et 29 mars 1985, Ottawa, Canada (ci-après désignée par CNVPI).

4. Taylor, R.C., "Trends in Data Integrity, Security and Use of Technology", Document de référence de la CNVPI, CNVPI, mars 1985, p. 13.

5. Exposé sur le projet de loi S-33, Loi sur la preuve au Canada, 1982, Comité des questions législatives et réglementaires canadiennes (CLARA), Comité sénatorial permanent des affaires juridiques et constitutionnelles, 23 juin 1983, Ottawa, pp. 2 et 3.

6. Tollefson, E.A., "Admissibilité en preuve des documents informatiques : Principes et problèmes", Document de référence de la CNVPI, mars 1985, p. 4.

7. Tollefson, p. 8.

8. Knoppers, Jake V. Th., "Résumé de la réunion plénière du 29 mars 1985", Note de la CNVPI aux participants, 3 juillet 1985.

9. Knoppers, Jake V. Th., "International Trade : The Information-Intensive Commercial Trends of the Future", document présenté au First International Records Management Congress, à Manille, du 18 au 22 novembre 1985, pp. 18-21. Publié dans le International Records Management Journal 3(1) (janvier 1987) : 21-27 et les trois numéros suivants.

CACC / CCAC
89645

QUEEN KE 5325 .K6614 1987 c.
Knoppers, Jake V. Th
Questions de droit que posen les

DATE DUE

Pour plus de détails, veuillez communiquer avec :

Le Centre canadien de recherche sur l'informatisation du travail
1575, boulevard Chomedey
Laval (Québec)
H7V 2X2
(514) 682-3400

For more information, please contact:

Canadian Workplace Automation Research Centre
1575 Chomedey Blvd.
Laval, Quebec
H7V 2X2
(514) 682-3400