Gouvernement du Canada
Ministère des Communications

Government of Canada
Department of Communications

Le Centre canadien de recherche sur l'informatisation du travail

Canadian Workplace Automation Research Centre

SÉCURITÉ DES DONNÉES EN BUREAUTIQUE

Exploration des questions et des préoccupations suscitées par le programme de la bureautique

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

QUEEN
P
91
.C655
K58314
1987

Queen
P
91
C655
K583
1987

COMMUNICATIONS CANADA
JUL 20 1987
LIBRARY – BIBLIOTHÈQUE

Industry Canada
Library Queen
JUL 2 1 1998
Industrie Canada
Bibliothèque Queen

SÉCURITÉ DES DONNÉES EN BUREAUTIQUE

Exploration des questions et des préoccupations suscitées par le programme de la bureautique

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

Centre canadien de recherche sur l'informatisation du travail

Ce document, révisé pour le Carrefour international sur l'information électronique, fût préalablement publié en 1984. Montréal, juin 1987 . Les opinions exprimées dans ce rapport n'engagent que l'auteur.

MCC-CCRIT-87-F-C03

P
91
C655
K58314
1987

DD 7350750
DL 7367425

PRÉFACE

Le présent rapport est une version légèrement modifiée d'un rapport établi en août 1984. par le Dr Knoppers à l'intention du ministère des Communications. On n'y a ajouté que quelques renseignements additionnels, car les conclusions du rapport demeurent valides.

Le rapport original était le résultat d'une série d'études faites par INFOMAN INC. sur les questions touchant la sécurité des données produites par le matériel bureautique. Ces études ont été demandées par la Division des programmes et des opérations de sécurité du ministère des Communication en tant qu'activité parallèle au Programme de la bureautique et venant appuyer ce dernier.

Ces études visaient à rationaliser une préoccupation importante reliée au développement de la haute technologie bureautique et à souligner au secteur public de même qu'au secteur privé la nécessité de s'attaquer à un problème potentiel créé par l'introduction de ces nouvelles technologies. Ce rapport devrait donc contribuer non seulement au travail d'élaboration et d'introduction des systèmes bureautiques, mais également à l'utilisation des systèmes bureautiques intégrés, en général.

On a ajouté une postface au rapport afin d'informer les lecteurs des plus récents progrès et activités ayant trait aux questions de sécurité et qui pourraient intéresser les lecteurs.

Enfin, notons que les participants au Carrefour international de l'information électronique peuvent consulter un autre rapport intitulé Questions de droit que posent les systèmes informatiques intégrés : Aperçu des considérations pratiques et des récents développements.

TABLE DES MATIÈRES

		Page
I.	SOMMAIRE	1
II.	INTRODUCTION	5
	A. HISTORIQUE	5
	B. OBJET ET PORTÉE	6
	C. MÉTHODOLOGIE	7
III.	LE PROGRAMME DE LA BUREAUTIQUE	10
	A. OBJET	10
	B. PORTÉE ET CONTENU INFORMATIONNEL	11
	C. QUESTIONS ET PRÉOCCUPATIONS DÉBATTUES AVEC LE PERSONNEL DU PROGRAMME DE LA BUREAUTIQUE	14
IV.	EXIGENCES DE SÉCURITÉ DES DONNÉES GÉRÉES PAR LE GOUVERNEMENT FÉDÉRAL	17
	A. LÉGISLATION RÉGISSANT LA SÉCURITÉ DES DONNÉES EN BUREAUTIQUE	17
	1. Introduction	17
	2. Loi sur l'accès à l'information	17
	3. Loi sur la protection des renseignements personnels	18
	4. Loi sur les secrets officiels	19
	5. Code criminel	20
	6. Loi sur la preuve au Canada	21
	B. CONSIDÉRATIONS RELATIVES À LA GESTION DE L'INFORMATION	22
	1. Introduction	22
	2. Politique du gouvernement sur la protection de l'information	22
	3. Politique de gestion de l'information	23
	C. REMARQUES SUR LES EXIGENCES RELATIVES À LA SÉCURITÉ DES DONNÉES EN BUREAUTIQUE AU GOUVERNEMENT FÉDÉRAL	27
V.	EXIGENCES DE SÉCURITÉ DES DONNÉES EN BUREAUTIQUE DANS LE SECTEUR PRIVÉ	35
VI.	CONCLUSIONS ET RECOMMANDATIONS	40
RÉFÉRENCES		47

I. SOMMAIRE

Le gouvernement fédéral procède actuellement à une série d'essais d'utilisation en milieu réel des technologies de bureautique, désignés comme le "Programme de la bureautique". Géré par le ministère des Communications, ce programme a pour objet principal de donner aux entreprises canadiennes de technologie de pointe l'occasion de démontrer leurs possibilités en bureautique et, par conséquent, de stimuler le développement industriel du Canada. Ce programme vise également un autre objectif très important, celui de s'attaquer aux questions et préoccupations reliées à l'implantation de la bureautique en milieu de travail, notamment en matière d'ergonomie, de qualité du travail, d'organisation ainsi que d'autres facteurs humains et sociaux.

Le Programme de la bureautique comprend cinq essais en milieu réel. Ces essais portent sur la transmission des données, de la parole, des graphiques, des textes et vidéo, par téléphone, par câble et par fibre optique, ainsi que sur l'introduction de postes de travail à fonctions multiples. La méthode adoptée consiste essentiellement à combiner les technologies de l'informatique et de la bureautique pour l'exécution de diverses tâches de traitement de l'information, à l'appui des fonctions de direction et d'administration. Il est question, entre autres, de remplacer autant que possible la technologie informatique en vigueur qui est basée sur l'impresssion (sur papier, sur microfilms, par copieur ou par télécopieur, etc.). Les essais en cours insistent sur l'application efficace de ces technologies et sur la recherche de moyens appropriés qui permettent aux travailleurs de s'adapter aux systèmes bureautiques et de les employer. Par conséquent, les considérations de gestion de l'information, en général, et celles de la sécurité des données concernant l'accès aux informations et l'usage de ces dernières, en particulier, sont passées au second rang et n'ont donc pas encore reçu l'attention qu'elles méritaient.

Le présent rapport expose une première étude sur les questions et les préoccupations relatives à la sécurité des données, en particulier celles qui ont trait à l'information confidentielle non reliée à la sécurité nationale, que suscite l'instauration de systèmes de bureautique au gouvernement fédéral. L'étude est fondée sur 1) des entretiens avec les gestionnaires des essais entrepris, 2) une analyse des politiques législatives, des directives et des lignes directrices, en vigueur ou envisagées pour la gestion et la protection de l'information, 3) une revue de la documentation existante, 4) l'ouvrage précédent de l'auteur concernant la gestion de l'information, la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels et 5) les questions de vulnérabilité des systèmes de communications et informatiques.

Voici les faits saillants et les éléments clés des entretiens avec les gestionnaires et autres agents des essais de bureautique :

- les applications courantes portent essentiellement sur les secteurs financiers et administratifs et n'englobent pas, en général, des informations confidentielles, bien que la portée de ces termes ne soit pas encore clairement définie;

- lorsque les utilisateurs sont familiarisés avec les technologies de la bureautique, ils auront naturellement tendance à s'en servir pour traiter tous les genres d'informations, y compris celles qui ont trait à la sécurité nationale et les informations confidentielles des autres secteurs;

- l'ajout ultérieur de fonctions de protection est difficile et coûteux;

- les mesures de sécurité des données devraient être intégrées aux systèmes bureautiques dès les premières étapes de la conception et de l'élaboration;

- il faut prendre davantage conscience de la nécessité de protéger certains genres d'informations, d'autant plus qu'on entrevoit une vague de nouveaux utilisateurs qui seront bien plus au courant des subtilités des systèmes;

- si les systèmes bureautiques deviennent complètement opérationnels et vraiment utiles, il faudra étudier de plus près les besoins en matière de sécurité des données.

Le présent rapport fait état de la législation fédérale régissant la sécurité, la confidentialité et la protection des renseignements personnels, de même que de politiques administratives actuelles ou à venir du gouvernement fédéral concernant l'usage des technologies informatiques et la gestion de l'information, y compris celles qu'entraînent la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels, en insistant particulièrement sur celles qui ont trait à la sécurité des données. D'après une étude préliminaire, dans l'optique de la sécurité des données, on voit clairement que ces dispositions s'appliquent également à l'information traitée par les systèmes bureautiques. Le rapport signale que les systèmes bureautiques et les procédures correspondantes doivent pouvoir répondre aux exigences des politiques administratives, juridiques et fédérales sur la communication et l'utilisation des informations s'ils doivent servir aux secteurs d'application les plus divers possibles.

Le rapport avance l'argument que la taille du marché de la bureautique et sa pénétration par les fournisseurs canadiens sont directement reliées à l'aptitude des systèmes bureautiques à traiter les informations confidentielles. Cette assertion est particulièrement vraie lorsque de tels systèmes sont employés pour accroître l'efficacité de la prise de décision par les gestionnaires supérieurs, plutôt que comme des instruments de productivité pour le cheminement des informations administratives ou courantes.

À cet effet, l'étude souligne tout d'abord le lien qui existe entre les besoins en bureautique du gouvernement fédéral et ceux du secteur privé pour pouvoir traiter les informations confidentielles. Elle démontre que si les fournisseurs canadiens prennent en considération l'aspect de la sécurité des données dans leurs soumissions, ils risquent d'accroître la valeur des produits bureautiques et leur pénétration dans le marché canadien et à l'étranger.

Le rapport se termine par les recommandations suivantes :

- l'établissement d'une série de lignes directrices et de procédures pratiques pour étendre aux systèmes bureautiques les exigences juridiques et administratives qui régissent actuellement l'accès à l'information et l'utilisation de celle-ci, sous la surveillance du gouvernement fédéral;

- la réalisation d'un projet pilote, qui comporterait peut-être un essai en milieu réel administré par le ministère des Communications, pour étudier les aspects pratiques des problèmes de sécurité des données et des préoccupations correspondantes que suscite l'utilisation de systèmes bureautiques;

- l'élaboration, à l'intention des fournisseurs canadiens, d'une série de documents qui exposeraient clairement et en termes pratiques les exigences en matière de sécurité des données que doivent respecter les systèmes bureautiques dans l'administration fédérale et qui préciseraient dans quelle mesure ces exigences sont semblables à celles du secteur privé.

II. INTRODUCTION

A. HISTORIQUE

Le ministère des Communications coordonne actuellement un certain nombre d'essais sur le terrain en bureautique. Cette initiative est désignée par le "Programme de la bureautique". Ce programme consiste à tester, dans certains organismes choisis, diverses combinaisons d'équipements produits par des fournisseurs canadiens, et ce, dans différents secteurs d'application. Les essais en questions comportent la transmission de graphiques, de la parole, vidéo et de textes par téléphone, par câble et par fibre optique, ainsi que la réalisation de postes de travail multi-fonctions.

Le principe du Programme de la bureautique consiste, d'une part, à fusionner les technologies informatiques et bureautiques et, d'autre part, à remplacer les technologies informatiques basées sur l'impression (sur papier, sur microfilms, par copieur, par télécopieur, etc.). Jusqu'ici, les essais sur le terrain effectués dans le cadre de ce Programme étaient axés sur la technologie même ainsi que sur la qualité du travail, sur l'ergonomie et sur d'autres facteurs humains et sociaux.

Le 1er juillet 1983, la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels étaient adoptées. Ces deux lois constituent en fait une nouvelle politique de traitement de l'information pour le gouvernement fédéral. Elle ne sont tributaires d'aucune technologie en particulier, c'est-à-dire qu'elle s'appliquent également à toutes sortes d'informations enregistrées et contrôlées par les organismes fédéraux, et elles précisent selon quels critères et dans quelles conditions l'information peut être révélée ou non.

Il existe également au gouvernement fédéral des politiques et des règlements qui prévoient la protection de certains renseignements contre leur révélation non autorisée. Parmi les nouvelles restrictions concernant

l'accès à l'information et la protection des renseignements personnels, un grand nombre ont été ajoutées aux politiques et règlements gouvernementaux en vigueur.

Le Programme de la bureautique et la bureautisation en général suscitent une question fondamentale, à savoir comment on applique la nouvelle politique de l'information (les deux lois susmentionnées) aux développements de la technologie informatique, tels que le Programme de la bureautique, et plus particulièrement comment on devrait réagir aux préoccupations que suscitent l'usage de ces technologies au gouvernement fédéral et les rapports qui existent entre cet usage et les objectifs du Programme de la bureautique à l'appui des développements du secteur privé. On n'envisage plus la bureautique comme jouant un rôle de gardien des centres de documentation ou de SIG. La bureautique doit être accessible à tous et être facile à utiliser. Ses systèmes sont portatifs. Ils combinent des éléments de gestion des enregistrements, de traitement électronique des données, de traitement de textes et de télécommunications, y compris leurs procédures et méthodes respectives.

En tenant compte de ces facteurs, la Division des programmes et opérations de sécurité du ministère des Communications a demandé à Infoman Inc. d'entreprendre une étude sur les questions de sécurité des données que soulève la bureautique. À ce chapitre, le présent rapport devrait faciliter le travail accompli en vertu du Programme de la bureautique et peut-être aider les organismes responsables de la direction et de l'orientation en gestion de l'information.

B. OBJET ET PORTÉE

Le présent rapport a pour but de déterminer les questions de sécurité des données que suscite la bureautique dans l'administration fédérale et de cerner, à titre préliminaire, celles qui se posent en même temps ou qui en résultent pour le secteur privé. Il n'aborde pas la question des informations reliées à la sécurité nationale, les mesures de protection

de ce genre d'informations ayant déjà été prescrites.

Ce rapport n'aborde pas non plus les questions sécuritaires reliées à l'utilisation accrue de la technologie de pointe, telles que la protection de l'équipement contre les abus ou le vol. Il n'en demeure pas moins que de telles questions ont leur importance et qu'elles devront être étudiées pour garantir l'accessibilité de l'équipement, en tant qu'élément intégral et essentiel de tout bureau automatisé.

Les trois chapitres qui suivent traitent tour à tour des trois volets du rapport. Le premier contient une analyse des essais en cours sur le terrain, à savoir leur domaine d'application, leur contenu informationnel et les discussions et entrevues correspondantes avec les participants.

Le deuxième passe en revue la législation existante, nouvelle et envisagée, les politiques de sécurité et de gestion de l'information gouvernementale ainsi que les documents connexes concernant la bureautique et la sécurité des données. Enfin, le but des essais en milieu réel étant d'aider les fournisseurs canadiens à développer leurs produits et services bureautiques, le troisième chapitre lance un débat préliminaire sur les liens entre les exigences en matière de sécurité des données au gouvernement fédéral et dans le secteur privé.

C. MÉTHODOLOGIE

Voici en quoi consiste essentiellement le travail :

- passer en revue les aspects suivants des essais de bureautique en milieu réel que le gouvernement fédéral effectue actuellement :

  - les objectifs du Programme de la bureautique,

- les domaines d'application et le contenu informationnel des essais en milieu réel et

- les entrevues avec les gestionnaires des essais en milieu réel et avec d'autres personnes sur les inquiétudes que suscite la bureautique au sujet de la sécurité des données;

- passer en revue les dispositions actuellement en vigueur au gouvernement fédéral, y compris celles des principales lois fédérales actuelles et envisagées, qui imposent une protection adéquate des renseignements d'une certaine nature pendant leur traitement, leur stockage ou leur transmission électronique, afin d'en préserver la confidentialité et

- déterminer, à titre préliminaire, les exigences de sécurité et de confidentialité en bureautique du secteur privé dont la nature ou la fonction sont semblables à celles du gouvernement fédéral.

L'étude a reçu pour titre "Sécurité des données". Ces termes englobent les notions de "sécurité", de "confidentialité" et de "protection des renseignements personnels" qui ont toutes des significations très différentes, et en général et sur le plan strictement technique.

Il serait donc utile de définir brièvement ces trois notions en ce qui a trait à la bureautique et à la gestion de l'information ainsi que dans le contexte du rapport.

Sécurité : il ne s'agit pas ici de la sécurité physique des ordinateurs ni du matériel de transmission et autre, ni de l'accès aux immeubles et aux bureaux. Ce terme désigne plutôt les mesures de sécurité logiques qui garantissent que seules les personnes autorisées peuvent accéder aux systèmes bureautiques et aux informations qu'ils contiennent. À ce titre, on entend par "sécurité" le contrôle de l'accès à l'information et les procédures nécessaires pour protéger celle-ci contre sa communication, sa destruction ou sa

manipulation non autorisées. Ce type de mesures de sécurité comprend les contrôles de l'entrée en communication, les codes d'accès, le rappel, le chiffrement, etc., c'est-à-dire des fonctions logicielles et de système.

Confidentialité : ce terme englobe les règles qui régissent la communication ou la non-communication de certaines informations stockées, bien déterminées et identifiables. En résumé, il désigne la nécessité de protéger les données contre leur communication non autorisée. Le principe de la révélation des seules informations indispensables au travail fait partie intégrante de la notion de confidentialité. L'obligation de garder confidentiels certains renseignements, stipulée dans la Loi et dans la politique du gouvernement, s'applique à différents niveaux et dans différents contextes, soit pour le public, par rapport au gouvernement seulement, au ministère seulement, au Cabinet seulement, aux tiers, à un groupe particulier de personnes participant à un programme déterminé (par exemple, recensement, impôt sur le revenu) ou à l'élaboration d'une nouvelle politique, etc. Les dispositions relatives à la confidentialité peuvent être fonction du poste de l'auteur du document, du niveau d'activité ou du contenu informationnel, etc., ou de toute combinaison de ces facteurs.

Protection des renseignements personnels : dans le contexte approprié, et en vertu de la Loi sur la protection des renseignements personnels, cette protection désigne une certaine série de règles concernant la création, le traitement, la transmission, la consultation et l'utilisation, la protection et la destruction des renseignements enregistrés sur des personnes ou reliés à ces dernières. Elle désigne également les exigences en matière d'exactitude et de confidentialité des données relatives à une personne, le droit d'accès d'une personne à ces données et l'assurance que les règles d'utilisation des données seront respectées. La protection des renseignements personnels est une notion relativement nouvelle et est devenue un nouveau droit de la personne avec l'avènement de l'ère de l'informatique.

Toutefois, les explications précédentes de ces trois termes ne sont que provisoires. D'autres efforts sont encore nécessaires pour en établir une définition théorique et pratique, surtout pour la notion assez nouvelle d'"intégrité des données". Par conséquent, dans ce rapport, l'expression "sécurité des données" est prise dans un sens collectif, parce qu'il est encore trop tôt pour établir si une question, une préoccupation ou une exigence particulière en bureautique relève de la sécurité, de la confidentialité, de la protection des renseignements personnels ou de l'intégrité des données, ou d'une combinaison de ces éléments.

III. LE PROGRAMME DE LA BUREAUTIQUE

A. OBJET

Le Programme de la bureautique est une initiative d'automatisation administrative du gouvernement fédéral, sous forme d'une série d'essais en milieu réel lancés et gérés par le ministère des Communications. Ces essais ont pour but de donner aux entreprises canadiennes de technologie de pointe l'occasion de démontrer leurs possibilités en bureautique et de stimuler ainsi le développement industriel au Canada. L'un des principaux buts du Programme est donc "d'aider l'industrie canadienne à satisfaire à la demande d'un marché appelé à devenir de plus en plus important, tant au Canada qu'à l'étranger".

Le Programme de la bureautique comporte un second objectif important : l'acceptation par les usagers de postes de travail multifonctions dans leur bureau ou autres lieux de travail. Aussi, le ministère déploie-t-il des efforts parallèles considérables, dans le cadre de ce Programme, pour s'attaquer aux questions et préoccupations reliées à l'ergonomie, aux facteurs organisationnels et à la productivité.

B. PORTÉE ET CONTENU INFORMATIONNEL

Des fonds fédéraux s'élevant à environ 12 millions de dollars ont été affectés aux essais de bureautique en milieu réel. La majorité de ces fonds serviront à procurer à cinq centres d'essais diverses combinaisons de matériel, de logiciel, d'installations de télécommunications, etc. mis au point par des fabricants canadiens. Les sommes restantes servent au financement des essais en milieu réel et à des études sur des questions telles que la performance du système, l'accueil fait par les usagers, les facteurs humains et sociaux, les aspects organisationnels et la productivité.

Les essais en milieu réel sont effectués dans les ministères suivants :

- ministère de la Défense nationale (Direction des services financiers, à Ottawa et à Winnipeg)

- Environnement Canada (Service de la protection de l'environnement et Services de gestion du ministère, à Ottawa-Hull et dans les régions)

- Revenu Canada (Accise) (Interprétation fiscales et gestion supérieure, à Ottawa-Hull et à Toronto)

- Énergie, Mines et Ressources (Services administratifs et Personnel, à Ottawa) et

- Communications Canada (Politique de radiodiffusion et de services connexes et Cabinet du ministre, à Ottawa)

Le secteur d'application de l'essai en milieu réel du ministère de la Défense nationale est la Direction des Services financiers, et les utilisateurs doivent être les agents des politiques et procédures financières du Quartier général du ministère ainsi que du quartier général du Commandement de l'air et de la Base des Forces canadiennes, tous deux à Winnipeg. Le contenu informationnel concerne essentiellement la

politique et l'administration financières. On y vise surtout le courrier électronique, la gestion des activités, la création et le classement des documents, l'indexation et l'extraction de l'information et l'utilisation des programmes de calcul de tableaux. Le système est déjà employé pour les messageries électroniques entre Ottawa et Winnipeg, concernant les erreurs commises dans les transactions relatives à la feuille de paye et au règlement automatique des factures.

À Environnement Canada, la première étape de l'essai en milieu réel se déroule à deux endroits, soit :

- à la Direction générale des Services de gestion du ministère et

- au Service de la protection de l'environnement.

Dans ce cas-ci, on insiste surtout sur le courrier et les messageries électroniques, la transmission de la parole, le traitement de textes, la gestion des activités et la gestion électronique de fichiers. On vise principalement à permettre aux usagers d'adopter le système en fonction des objectifs qu'ils jugent utiles. Au service de la protection de l'environnement, le système est destiné aux gestionnaires supérieurs et moyens, alors qu'à la Direction générale des services de gestion, il est davantage destiné aux gestionnaires moyens et subalternes, ainsi qu'au personnel administratif et de soutien.

À Revenu Canada (Accise), le domaine d'application de l'essai en milieu réel est celui des gestionnaires supérieurs de l'Accise, à Ottawa et à Toronto, dans le secteur des Interprétations fiscales et dans un groupe de gestion. L'essai vise surtout les services intégrés de transmission de la parole et des données, les services téléphoniques de pointe, la transmission de textes et le traitement des documents. Quant au contenu informationnel, il s'agit principalement des interprétations fiscales courantes, des procédures de soutien administratif de la documentation, de la création et de l'acheminement des formules, de même que de l'établissement des calendriers et des programmes journaliers des participants.

L'un des buts de l'essai consiste à assurer l'accès individuel en direct aux bases de données juridiques.

L'essai en milieu réel à Énergie, Mines et Ressources est axé sur l'extraction et le classement électronique, au Secteur finances et administration. Le principal contenu informationnel de cette application du Programme réside dans les manuels de la politique administrative du ministère.

Au ministère des Communications, le Programme porte sur le secteur de la politique de la Direction générale des politiques de radiodiffusion et de services connexes, ainsi que sur les cabinets du ministre, du sous-ministre et du sous-ministre adjoint principal. Bien que le courrier électronique et la correspondance ministérielle occupent une place spéciale dans cette application, celle-ci comprend également d'autres fonctions telles que le traitement de textes, le Télidon, les programmes de calcul de tableaux financiers, les communications et l'accès des terminaux éloignés aux serveurs de fichiers centraux.

En résumé, les essais de bureautique en milieu réel sont axés sur l'évaluation des problèmes techniques que présentent les différentes combinaisons de composantes de création canadienne et sur l'étude de questions particulières reliées à l'introduction des nouveaux systèmes et technologies informatiques dans le lieu de travail. Les principaux secteurs d'application sont le courrier et les messageries électroniques, l'établissement de calendriers et la gestion des activités, le traitement de textes, le calcul de tableaux financiers, les politiques et procédures administratives et financières, etc. Le contenu informationnel prévu des essais en cours est ainsi surtout de nature administrative. Cependant, l'essai en milieu réel entrepris à Revenu Canada (Accise) inclut la participation du groupe des Interprétations fiscales, et celui du ministère des Communications vise surtout l'accélération de la correspondance ministérielle, de la présentation de mémoires au Conseil du Trésor, de l'établissement des rapports et de l'analyse des politiques, etc.

L'essai en milieu réel de ÉMR porte spécialement sur l'information mise à la disposition du public, en envisageant l'accès en direct au système autonome.

Dans plusieurs essais, il a été décidé de ne pas confier aux prototypes du Programme de la bureautique le traitement d'informations confidentielles. Toutefois, à mesure que les utilisateurs se familiarisent avec leurs systèmes bureautiques, on s'attend à ce qu'ils tendent progressivement à s'en servir autant que possible et à ce qu'ils désirent être en mesure de pouvoir traiter tous les genres d'informations.

C. QUESTIONS ET PRÉOCCUPATIONS DÉBATTUES AVEC LE PERSONNEL DU PROGRAMME DE LA BUREAUTIQUE

Lors des entretiens avec les gestionnaires de projet et autres agents participant aux essais en milieu réel, un certain nombre de sujets ont été débattus concernant les caractéristiques ou exigences relatives à la sécurité des données qui s'appliquent à la bureautique ou qui en résultent. Voici un résumé de ces sujets.

- En substance, tous les essais en milieu réel comportent des contrôles d'accès et d'entrée en communication. En outre, des mesures sont prévues pour distinguer les fichiers ou documents "publics" ou collectifs, y compris les documents centraux, des documents "privés" ou personnels, c'est-à-dire ceux qu'on dépose dans son propre bureau. La plupart de ces essais ne prévoient pas de contrôles d'accès ou des degrés de sécurité distincts au niveau du fichier ou du document. Seul Environnement Canada fait exception, le système de l'essai en milieu réel étant conçu avec des contrôles d'accès au niveau de l'élément d'information.

- Selon les observations de plusieurs interlocuteurs, du point de vue de la sécurité des données, il n'est pas toujours possible de faire une partie de son travail d'une façon et le reste d'une autre façon. En

d'autres termes, une fois qu'on se familiarise avec l'utilisation de systèmes bureautiques et qu'on commence à compter sur eux pour le travail quotidien, on tend à s'en servir pour traiter aussi bien les informations confidentielles que les autres. Ils ont cité, à titre d'exemple, l'expérience du traitement de textes.

- Auparavant, les mesures de sécurité des documents imprimés résidaient en partie dans les contraintes physiques et de volume, c'est-à-dire qu'il aurait fallu à une personne non autorisée beaucoup de temps pour parcourir tous les documents d'un classeur afin d'y trouver quelque chose d'intéressant; la chose ne serait donc pas passée inaperçue. Avec la technologie et les systèmes bureautiques, qui sont d'un usage facile, le degré de risque et de vulnérabilité est tout autre, parce qu'on peut explorer très vite ou de très loin, et sans se faire remarquer, des volumes considérables de documents, à la recherche de renseignements "intéressants". On pourrait copier des documents sans qu'ils n'aient jamais quitté les archives ou qu'ils n'aient "disparu" du dossier. Il est également possible de modifier électroniquement des documents sans laisser de traces de modifications qu'on aurait détectées sur les documents de papier.

- Dépendance à l'égard du système - Si la bureautique réussit et qu'on laisse tomber le système parallèle d'impression sur papier, faudra-t-il tous les jours une copie de sauvegarde? Qu'arrivera-t-il si quelqu'un altère le système? Qu'arrive-t-il si un document électronique est mal classé? Dans un système basé sur des documents de papier, on finit par voir un document mal classé et par le reclasser, mais dans un système bureautique, un document mal classé pourrait être perdu à jamais.

- Ceux qui connaissent bien les systèmes informatiques et de transmission ont signalé que le recyclage d'un système bureautique en fonction d'une série de normes de sécurité des données exige énormément de fonds, d'années-personnes et de temps. La conception de certains systèmes rend parfois impossible un tel recyclage. Les interviewés

étaient d'avis que les aspects de la sécurité des données devraient être pris en considération dès le début dans les systèmes bureautiques, soit aux étapes de la planification, de la conception, de l'essai et de la mise en oeuvre.

- Sur un plan plus général, l'arrivée prévue de toute une vague d'utilisateurs "experts" dans la fonction publique, conjuguée avec la facilité d'utilisation et la portabilité croissante des systèmes et de l'équipement bureautiques, était considérée à la fois comme un sujet d'inquiétude et comme une bonne raison pour prévoir des politiques et des procédures de sécurité des données en bureautique, y compris l'étude de ce qui constitue un comportement contraire à l'éthique.

IV. EXIGENCES DE SÉCURITÉ DES DONNÉES GÉRÉES PAR LE GOUVERNEMENT FÉDÉRAL

A. LÉGISLATION RÉGISSANT LA SÉCURITÉ DES DONNÉES EN BUREAUTIQUE

1. Introduction

La présente section contient une étude préliminaire, du point de vue de la bureautique, des principaux lois et règlements en vigueur ou prévus qui exigent que l'information d'une certaine nature soit adéquatement protégée lorsqu'elle est traitée électroniquement, afin d'en préserver la confidentialité. Parmi les lois fédérales qui imposent des restrictions à l'accès à certaines informations enregistrées ainsi que la protection des renseignements confidentiels, on peut citer la Loi de l'impôt sur le revenu, la Loi sur la statistique, le Régime de pensions du Canada, la Loi sur les casiers judiciaires et la Loi sur les allocations familiales. Ce chapitre portera non pas sur des lois particulières à un organisme ou à un programme déterminé du gouvernement, mais plutôt sur les principales lois qui concernent tous les organismes du gouvernement et, par conséquent, toutes les applications de bureautique.

- la Loi sur l'accès à l'information;
- la Loi sur la protection des renseignements personnels;
- le Code criminel;
- la Loi sur les secrets officiels;
- la Loi sur la preuve au Canada.

2. Loi sur l'accès à l'information

Cette loi, adoptée le 1er juillet 1983, donne aux Canadiens le droit d'accès à des informations gérées par le gouvernement fédéral, y compris celles qui se présentent sous forme compréhensible par la machine. Il s'ensuit que toute information ou combinaison possible de données pouvant être extraite d'un système bureautique est soumise à cette Loi.

Toutefois, la Loi prévoit plusieurs domaines où l'information ne peut être communiquée ou peut l'être sous réserve d'examen. Par le truchement de ces exceptions et de la stipulation de contraintes sur la communication de certaines informations, la Loi contient une série de critères qui permettent de déterminer les aspects de la sécurité des données à étudier.

Le gouvernement est maintenant juridiquement tenu d'adopter des mesures de sécurité des données qui soient conformes à l'esprit de la Loi sur l'accès à l'information.

3. Loi sur la protection des renseignements personnels

Cette Loi est une version révisée et enrichie de la Partie IV de la Loi canadienne sur les droits de la personne. Elle a étendu la définition des "renseignements personnels" et clarifié certains des droits prévus. Cette Loi a été adoptée le 1er juillet 1983.

En principe, le droit à la protection des renseignements personnels exige que les renseignements directs ou indirects sur les personnes soient disponibles en temps opportun, exacts et pertinents; qu'ils soient détruits lorsqu'on n'en a plus besoin; que les renseignements rassemblés ou enregistrés au sujet des personnes soient limités, destinés à un but ou à un usage bien défini et, autant que possible, soient obtenus directement auprès de l'intéressé; que celui-ci ait le droit de savoir quelles données existent sur lui, qui les a rassemblées et qui les utilise ou les enregistre; qu'il ait également le droit d'accéder (sauf dans le cas d'exceptions bien déterminées) à des renseignements personnels, qu'il puisse en vérifier l'exactitude et la pertinence et demander la suppression, l'addition ou la correction de telles données et que, en cas de conflit, il ait le droit d'en appeler à un tiers neutre, comme le Commissaire à la protection de la vie privée.

À ce titre, la Loi sur la protection des renseignements personnels, comme la Loi sur l'accès à l'information, expose les critères de communication, d'utilisation et de confidentialité des renseignements sur les personnes, y compris ceux qui sont conservés par n'importe quel système bureautique. En résumé, tout système de ce genre employé par un organisme fédéral et contenant des renseignements personnels doit pouvoir garantir que les dispositions juridiques de la Loi sur la protection des renseignements personnels seront respectées.

4. Loi sur les secrets officiels

Jusqu'à l'adoption de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, la Loi sur les secrets officiels était la seule loi d'application universelle à servir de base aux règlements et politiques gouvernementales visant à garantir que les renseignements qui ne devaient pas être divulgués ne le seraient effectivement pas. La Loi exige également que les fonctionnaires prêtent serment de discrétion. Cependant, pour le moment et dans l'avenir immédiat, il semble que la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels prévalent pour la détermination des critères généraux et détaillés de sécurité des renseignements contenus dans les systèmes bureautiques. De plus, la Loi sur les secrets officiels envisageait la sécurité des renseignements avant tout dans l'optique de la sécurité nationale. La Loi sur l'accès à l'information prévoit un certain nombre de restrictions, discrétionnaires et obligatoires, de l'accès à des catégories d'information qui n'intéressent pas forcément la sécurité nationale, mais qui demeurent confidentielles et qu'on ne doit donc pas communiquer sans autorisation, prématurément ou sans contrôle.

5. Le Code criminel

Le 7 février 1984, un bill omnibus prévoyant des modifications au Code criminel, le Bill C-19, était soumis à la Chambre des communes. Pour les besoins de la présente étude, il convient de noter deux des modifications proposées, concernant la fraude informatique et l'abus des données. Si ces deux modifications sont adoptées, l'utilisation des technologies informatique et de transmission ainsi que des autres composants bureautiques pour le traitement des données confidentielles sera réglementée par la loi.

Dans le contexte de la bureautique en particulier et de l'informatique et de la transmission en général, il faut élaborer des procédures de sécurité des données pour qu'en cas d'infraction, surtout de divulgation de renseignements confidentiels, on puisse porter une accusation en vertu du Code criminel, indépendamment de la Loi sur l'accès à l'information ou de la Loi sur la protection des renseignements personnels.

À cet effet, il faudrait au moins pouvoir démontrer que l'utilisateur d'un système bureautique était tout à fait conscient et bien informé de ce qui constitue un comportement "criminel" dans l'utilisation de pareils systèmes. Il faudrait également élaborer, à l'intention de l'usager, une série d'instructions très claires sur l'emploi des systèmes bureautiques, y compris des mesures techniques et procédurales particulières, pour que les utilisateurs soient conscients des exigences de sécurité de données et qu'ils aient aussi reçu la formation nécessaire pour les appliquer. Si ces précautions ne sont pas prises, il pourrait être difficile de mettre la question en litige lorsque les modifications proposées sur la fraude informatique et l'abus des données entreront en vigueur.

À noter qu'en vertu de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, ainsi que de la politique du Conseil du Trésor, la communication sur demande d'informations ne constitue pas une infraction aux termes de la présente Loi sur les secrets officiels. Cependant, le recours aux nouvelles peines proposées, en vertu du Code criminel, pour l'abus des données, serait encore possible si les systèmes bureautiques étaient en cause dans la divulgation non autorisée de renseignements confidentiels ou personnels et si l'utilisateur de tels systèmes avait été mis au courant de la définition du "comportement non autorisé".

6. Loi sur la preuve au Canada

On reconnaît que l'une des raisons pour lesquelles de nombreux organismes hésitent à se convertir entièrement à la bureautique est l'incertitude qui entoure l'acceptabilité des documents générés par ordinateur à titre de preuve devant les tribunaux. Par conséquent, toute modification de la Loi sur la preuve qui reconnaîtrait l'acceptabilité de tels documents, y compris ceux qui seraient produits par suite d'une mise en litige, éliminerait un sérieux obstacle à l'expansion de la bureautique dans des domaines d'application possibles beaucoup plus nombreux encore.

Actuellement, le projet S-33 de Loi uniforme sur la preuve représente une tentative pour rendre les lois sur la preuve adaptées aux technologies informatiques modernes, en y ajoutant un article sur la preuve enregistrée qui prévoirait l'acceptabilité dans les tribunaux des enregistrements générés par ordinateurs. Une fois adoptée, la Loi accélérerait considérablement la bureautisation, surtout dans le secteur privé, élargissant ainsi la taille et la portée du marché de la bureautique au Canada. L'une des grandes ramifications de la loi proposée est que cette modification de la Loi sur la preuve exigerait également que les systèmes bureautiques puissent démontrer l'intégrité des données en question.

B. CONSIDÉRATIONS RELATIVES À LA GESTION DE L'INFORMATION

1. Introduction

L'objet de la présente section est double. D'une part, on examine les politiques gouvernementales sur la protection de l'information et, d'autre part, on y passe en revue les politiques, directives et lignes directrices relatives à la gestion de l'information dans l'administration fédérale. On verra en particulier les politiques relatives aux préoccupations en matière de sécurité des données ainsi que leur application à la bureautique ou leur rapport avec cette dernière.

2. Politique du gouvernement sur la protection de l'information

La politique du gouvernement fédéral sur la sécurité de l'information est exposée dans le document intitulé "Sécurité de l'information dans la Fonction publique du Canada", publié d'abord en 1956 par le Conseil privé du Canada, puis révisé en 1977-1978. Ce document visait l'uniformisation en matière d'identification, de classification et de protection des informations confidentielles du gouvernement, son objet le plus important étant de veiller à ce que tous les fonctionnaires soient informés des exigences correspondantes et agissent en conséquence. Le document expose un système de classification à quatre niveaux ainsi qu'une série de procédures à suivre pour garantir le maintien d'un niveau de sécurité approprié, afin de protéger l'information selon sa valeur pour une puissance étrangère et selon l'étendue du préjudice ou des atteintes que sa communication non autorisée causerait à la nation.

Certains principes de cette politique de sécurité sont encore valides, mais on peut s'interroger sur l'applicabilité de cette dernière à la bureautique; aussi, nombreux sont ceux qui considèrent ce document comme inadéquat compte tenu des préoccupations actuelles en matière de sécurité et de nouvelles technologies de l'information. Néanmoins, les informations classées comme vitales pour la sécurité nationale ne

peuvent être traitées, transmises ou manipulées électroniquement sans que des mesures spéciales ne soient prises pour les protéger contre des fuites compromettantes et pour prévenir toute surveillance indésirable. C'est pour ces raisons que de telles informations ont été exlues de tous les essais en milieu réel.

Il n'en demeure pas moins qu'on a besoin de confier aux systèmes bureautiques le traitement d'informations confidentielles en assurant un niveau de sécurité des données approprié. Il en est ainsi surtout pour les secteurs où la bureautique doit servir à accroître l'efficacité de la prise de décisions par les cadres supérieurs (plutôt que la productivité, comme dans le secteur administratif).

3. Politique de gestion de l'information

Dans la mesure où la bureautique représente une tentative d'intégration de technologies de l'information jusqu'ici distinctes, il a été jugé utile de revoir brièvement les chapitres de "Gestion de l'information", Manuel de la politique administrative (MPA) du Conseil du Trésor, dont certaines sections permettraient de déterminer les préoccupations que suscite la bureautique au sujet de la sécurité des données.

Pour aider les organismes gouvernementaux à mettre en oeuvre et à administrer la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels, et en vertu de ces mêmes lois, le Conseil du Trésor a émis en juin 1983 les Lignes directrices provisoires : Loi sur l'accès à l'information et Loi sur la protection des renseignements personnels (chapitre 410, MAP). Ce chapitre explique les dispositions juridiques des deux lois et prescrit les méthodes que les organismes du gouvernement doivent suivre pour s'y conformer.

Du point de vue de la sécurité des données, ces lignes directrices jettent les fondements de l'application des exceptions qui régissent le refus de la communication des documents du gouvernement ainsi que la

protection des renseignements personnels, de même que l'utilisation et la communication de tels renseignements. Dans ce guide, il est clair que c'est maintenant dans le cadre de la Loi sur l'accès à l'information, qui indique quels renseignements peuvent être communiqués et lesquels ne doivent pas l'être, qu'il faut organiser l'information et considérer les préoccupations au sujet de la sécurité des données.

La Partie III (Vie privée) des Lignes directrices provisoires est émise en vertu et de la Loi sur la protection des renseignements personnels et de la Loi sur l'administration financière. Le but essentiel de cette politique est de protéger les renseignements personnels, c'est-à-dire d'en restreindre la collecte, la conservation et l'élimination, aussi bien que l'usage et la communication. Par "renseignements personnels", il faut entendre toute information enregistrée relative à une personne ou qui pourrait identifier une personne. Il y a lieu, par conséquent, d'intégrer aux technologies bureautiques les principes généraux de la Loi sur la protection des renseignements personnels, soit les principes d'exactitude, de pertinence, d'intégralité et d'opportunité, y compris les procédures appropriées de sécurité des données, en vue de la mise en oeuvre de cette directive.

Alors que le chapitre 410 exposait les directives et lignes directrices de la politique sur la communication et l'utilisation de l'information, les chapitres des séries 430, 440 et 450 traitent de l'usage des technologies informatiques.

Les chapitres 435 et 436 traitent de l'usage des technologies des télécommunications au gouvernement fédéral. En particulier, ils exposent les politiques et les procédures de gestion, d'administration et d'acquisition des biens et services de télécommunications et établissent les responsabilités et les exigences en matière de protection des données touchant la sécurité nationale et des autres informations confidentielles.

Le chapitre 440 traite des politiques et procédures de traitement électronique des données. Il a été modifié et révisé en décembre 1978 et s'applique maintenant à tous les équipements, les services et le personnel informatiques employés à des fins générales au gouvernement. Alors que ce chapitre ne désigne pas expressément la bureautique, les principes qu'il exprime s'y appliquent. Ce chapitre reconnaît l'importance toujours croissante des systèmes informatiques et prévoit que la gestion actuelle de l'informatique dans les ministères soit fondée sur les procédures courantes de planification et d'approvisionnement, y compris les méthodes et les mécanismes relatifs à la sécurité et au contrôle. La section 8 de ce chapitre traite spécialement de la sécurité informatique et constitue un élément clé de la politique pour ce qui a trait à la sécurité des données en bureautique. En outre, selon une directive énoncée dans cette section, les organismes du gouvernement doivent veiller à ce que les renseignements, quelle qu'en soit la forme, dont ils sont responsables reçoivent le niveau de protection prescrit pour leur classe sécuritaire ou leur degré de confidentialité.

Bien que ces chapitres aient été publiés il y a quelque temps déjà, ils prévoient, dans une certaine mesure, l'inclusion de la bureautique et le fait que les politiques informatiques et de télécommunications devraient très souvent être traitées non pas comme des secteurs distincts, mais plutôt comme faisant partie intégrante des autres. Les politiques énoncées dans ces chapitres semblent faire déjà état du besoin de sécurité des données et, par conséquent, exigent qu'on tienne compte des facteurs appropriés, surtout des facteurs techniques, lorsqu'on instaure des systèmes bureautiques dans les organismes du gouvernement fédéral.

Enfin, les lignes directrices contiennent une série de chapitres sur la gestion de l'information enregistrée. Parmi ces chapitres, le chapitre 460 traite de la gestion des documents imprimés, c'est-à-dire des supports physiques sur lesquels l'information est enregistrée, alors que le projet de chapitre 461 aborde la gestion des données, c'est-à-dire la gestion de l'information, quel que soit le support physique sur lequel elle est enregistrée.

Le chapitre 460 a été révisé et réédité par le Conseil du Trésor en mars 1983. Il contient la première d'une série de politiques sur l'information destinées à aider les ministères et les organismes à mettre en oeuvre les lois sur l'accès à l'information et sur la protection des renseignements personnels. L'un des principaux objectifs de ce chapitre est de garantir que les documents seront protégés contre l'accès, la divulgation et la modification non autorisés ainsi que contre la destruction et la perte. Ce chapitre traite de la gestion des documents du Cabinet d'un ministre, y compris les documents personnels et ceux du ministère. Il exige que, dans tout système d'archives :

- les documents du ministère soient inclus à titre de sous-ensembles du système de classification des dossiers par sujet de ce ministère et

- ces documents soient séparés des documents personnels du ministre.

Ce même chapitre sur la politique exige que les renseignements confidentiels du Cabinet constituent un sous-ensemble distinct de renseignements et soient protégés contre l'accès non autorisé, conformément aux procédures supervisées par le vérificateur de la sécurité des documents du Cabinet, au bureau du Conseil privé et, pour ce qui a trait aux documents du Conseil du Trésor, par le bureau du secrétaire du Conseil du Trésor.

On propose de substituer le chapitre 461, concernant la Gestion des données informatiques, à l'ancien chapitre 440.7, Informatique : gestion des archives. Ce chapitre 461 existe actuellement sous forme de projet seulement et est censé couvrir la gestion des informations enregistrées sous une forme et d'une manière qui conviennent à la communication, à l'interprétation ou aux traitements automatiques. D'après ce projet, les organismes du gouvernement doivent élaborer des procédures internes pour régir des questions précises, telles que :

- la protection des renseignements personnels, c'est-à-dire la vie privée,

- la classification des données assimilables par la machine, selon le préjudice susceptible de résulter de leur divulgation,

- le stockage, la manipulation, la transmission, le transfert et la destruction des informations compréhensibles par la machine et ayant une cote sécuritaire, et

- la déclassification des données ayant une cote sécuritaire.

C. REMARQUES SUR LES EXIGENCES RELATIVES À LA SÉCURITÉ DES DONNÉES EN BUREAUTIQUE AU GOUVERNEMENT FÉDÉRAL

Il est clair que la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels ainsi que les règlements, directives du CT et politiques administratives correspondantes s'appliquent à l'information manipulée par les systèmes bureautiques. De même, on souligne l'applicabilité de ces dispositions en particulier à toutes les informations nouvellement enregistrées ainsi qu'à tous les nouveaux systèmes basés sur les technologies de l'ordinateur, des communications et de l'information. Pour la première fois, les nouvelles politiques sur l'information offrent un cadre de travail et des critères juridiques parfaitement clairs pour l'octroi et la restriction du droit d'accès aux informations du gouvernement.

En fait, les responsabilités statutaires du contrôle de la communication et de l'usage des informations confidentielles sont maintenant nettement définies.

Si l'un des objectifs de la bureautique consiste à favoriser et à accroître l'efficacité de la prise de décisions, les gestionnaires supérieurs doivent pouvoir se servir des systèmes bureautiques. Ceux-ci doivent donc pouvoir satisfaire aux exigences de sécurité concernant les documents ministériels, ceux du Cabinet ainsi que les renseignements confidentiels du Conseil privé de la Reine.

Les exigences suivantes présentent un intérêt particulier dans le contexte de la bureautique :

- les documents confidentiels du Cabinet doivent être clairement estampillés à ce titre par leur auteur

- les renseignements confidentiels du Cabinet doivent être séparés des autres documents portant sur le même sujet

- il faut tenir un registre distinct des fichiers qu'on sait contenir des renseignements confidentiels du Cabinet, pour garantir leur retrait au cas où des personnes non autorisées à y accéder examineraient les dossiers et

- les jaquettes de fichiers ou les serviettes contenant de tels renseignements confidentiels du Cabinet doivent porter clairement à l'extérieur une marque indiquant qu'elles contiennent des renseignements confidentiels du Cabinet.

On met déjà en application des exigences pour les documents imprimés, par l'usage de fichiers et de systèmes de classement distincts ainsi que de codes de couleurs pour les fichiers et l'estampillage des documents personnels, etc. Si les systèmes bureautiques doivent contenir des documents de ce genre, et ils le devront sûrement pour devenir un instrument de soutien efficace dans la prise de décisions des cadres supérieurs, il leur faudra répondre à ces exigences opérationnelles et de sécurité des données.

Dans ce contexte, il faut remarquer par ailleurs qu'un grand nombre, pour ne pas dire la plupart, des renseignements confidentiels du Cabinet ne touchent pas la sécurité nationale, mais ont trait aux politiques, programmes et initiatives sociales et culturelles du pays (sur les plans national, régional et local) ainsi qu'aux dépenses correspondantes de fonds fédéraux (p. ex. un programme régional de travail ou d'encouragement, une initiative culturelle, des projets de changements au code criminel concernant le divorce, etc.). Par conséquent, une question importante se pose : comment distinguer et séparer les documents confidentiels du Cabinet, comme l'exigent les règlements sur l'accès à l'information, dans les systèmes bureautiques et comment protéger de tels documents contre leur communication par inadvertance ou sans autorisation.

Alors que les politiques et les méthodes sécuritaires courantes qui s'appliquent aux télécommunications, à l'information, au traitement de textes, à la gestion des documents et des données, etc. ne traitent pas particulièrement des systèmes bureautiques, les principes, eux, demeurent les mêmes. Voici, cependant, les principaux problèmes qui se posent :

a) quelle combinaison des politiques, lignes directrices et procédures en vigueur convient particulièrement à la bureautique et comment peut-on l'appliquer;

b) quelles sont les nouvelles questions et préoccupations que suscite la bureautique à l'endroit de la sécurité des données et quel est le meilleur moyen d'y faire face.

Voici quelques exemples parmi d'autres des problèmes particuliers à la bureautique et aux inquiétudes qu'elle suscite au sujet de la sécurité des données : les utilisateurs pourront-ils facilement éliminer et retirer des fichiers? À quel moment un "projet" devient-il document du gouvernement et ne peut être détruit sans autorisation? Lorsqu'un document est créé et classé dans un système bureautique, ne serait-ce que sous forme de projet, n'est-ce pas là le moment où entrent en jeu les considérations de sécurité des données?

En matière de gestion des documents, un dossier est essentiellement un contenant destiné à recevoir un groupe de documents, alors qu'en bureautique, un fichier ou un nom de fichier est souvent attribué à un seul document (document, lettre, rapport, etc.). De même, pour les documents de papier, les méthodes de sécurité fonctionnent essentiellement au niveau des "documents se trouvant dans un fichier", les chemises portant une marque spéciale et pouvant contenir et contenant souvent à la fois des renseignements confidentiels et d'autres qui ne le sont pas. Les principes et méthodes qui permettent d'identifier clairement les renseignements confidentiels au niveau de la chemise ou du document de papier devront être convertis en lignes directrices et méthodes pour les systèmes bureautiques. Il serait utile de déterminer les relations entre la gestion des documents et la bureautique, ainsi que les liens de cette gestion avec les facteurs de sécurité des données prévus par la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels.

La politique de gestion de l'information du gouvernement (section 460.6.5), plus exactement sur les documents essentiels, exige que les établissements déposent un ensemble de documents essentiels dans des lieux sûrs administrés par les Archives publiques. Dans le cas des documents de papier, on peut ajouter les microfilms et, dans celui des opérations traditionnelles ou du traitement de gros volumes de données, on peut ajouter les bandes de sauvegarde périodique et les vidages de bases de données. Toutefois, il y a lieu de se demander si ces exigences doivent être appliquées à la bureautique. Les systèmes bureautiques sont considérés comme très dynamiques en ce qui concerne les modifications du contenu informationnel et consistent en diverses structures et configurations de matériel, de logiciel et de données. Ces systèmes sont un véritable défi pour ce qui a trait aux documents essentiels.

La politique de gestion des documents du gouvernement stipule également que l'établissement et l'application de calendriers de conservation des documents doivent se faire au niveau du fichier. Dans les systèmes bureautiques, il est peut-être plus pratique de ramener la

classification et la déclassification sécuritaires, les calendriers de conservation et l'élimination, etc. au niveau du document, ou même au niveau de l'élément d'information, au moyen de règles de contrôle strictes comparables à celles qui régissent actuellement les opérations manuelles.

En outre, la Section 440.8.5.6 précise que l'auteur des données à traiter devrait déterminer et indiquer clairement la cote sécuritaire des données, s'il y a lieu. Dans le contexte de la bureautique, il faudrait à cet effet inclure une fonction qui permettrait à l'utilisateur d'étiqueter les documents ou les fichiers pour indiquer le degré de sécurité applicable, de même que le logiciel et les autres fonctions techniques nécessaires pour réaliser une application particulière. À un moment donné, il faudrait également prévoir un moyen pour que l'utilisateur passe ou fasse appel à un mode plus sûr dans un système bureautique. De même, les mesures de contrôle que comportent les systèmes bureautiques pour la saisie, le traitement, la sortie, etc. des données devraient inclure des éléments appropriés pour la sécurité des données.

L'étude de la politique actuelle du gouvernement sur la protection de l'information ainsi que des procédures de sécurité courantes relatives aux renseignements confidentiels imprimés a suscité certaines préoccupations au sujet de la bureautique et de la sécurité des données. Il serait utile d'en citer un certain nombre dans le présent rapport.

- Dans le secteur de la déclassification, et étant donné que le facteur du temps de communication de renseignements est souvent important, l'utilisation des systèmes bureautiques permettra-t-elle de réduire automatiquement la cote des documents après un délai déterminé, une date précise ou le déroulement d'un événement particulier?

- Lorsqu'il s'agit de documents confidentiels sur papier, les exemplaires en sont numérotés. En bureautique, comment prévenir la reproduction non autorisée d'un affichage? L'accès aux programmes de déchiffrement sera-t-il réservé à certains utilisateurs?

- Quelle sera la version bureautique du principe de la "mise sous scellé" et de l'usage du double pli cacheté? Ou celle du reçu signé d'un document? Ou encore celle de la vérification de signature?

- Comment traduira-t-on en bureautique l'exigence que les combinaisons de serrures de classeurs soient modifiées tous les six mois, au départ d'employés ou lorsque les combinaisons sont compromises (p. ex. les codes d'accès ou les mots de passe seront-ils modifiés tous les six mois)? À quels intervalles devrait-on réexaminer les profils des usagers? Faudra-t-il changer les mots de passe de tous ceux qui sont reliés au départ d'un employé, p. ex. d'une secrétaire ou d'un agent administratif qui travaille pour plusieurs personnes?

- Comment sera appliqué en bureautique le principe du "besoin de connaître"? Faudrait-il l'intégrer au profil d'accès de l'utilisateur? Ou encore au profil d'accès au document?

- La portabilité des micro-ordinateurs et des disquettes conduira-t-elle à des cas où des agents apporteraient des renseignements personnels chez eux?

- Comment traduira-t-on l'exigence que tous les document confidentiels soient déposés en lieu sûr, sous clé, la nuit, dans un contexte bureautique où l'application en jeu est disponible en direct 24 heures par jour? Et accessible de loin ou de chez soi? Ou encore si ces documents résident sur un support qu'on ne peut déplacer?

- S'il s'agit d'emporter des documents confidentiels chez soi, dans des contenants sous clé, la version bureautique consisterait-elle à emporter des chargeurs pouvant être bloqués? Et qu'en est-il de l'exigence d'inscrire en entrée et en sortie de tels documents confidentiels? Comment va-t-on concilier de telles exigences avec l'objectif des systèmes bureautiques qui consiste à permettre l'accès direct, par simple téléphone, de n'importe où au Canada (ou au monde)?

En ce qui concerne l'information et la formation de l'utilisateur en matière de sécurité des données en bureautique, une stratégie fondée sur l'analogie avec les documents imprimés pourrait être la plus productive. L'objet de la bureautique étant que les systèmes soient d'un usage facile et n'exigent donc pas de connaissances techniques particulières, l'acpect humain, qui consiste à garantir la protection des renseignements confidentiels, constitue le plus grand défi à relever.

Enfin, l'exigence de sécurité des données en bureautique devra tenir compte des politiques de sécurité en vigueur, comme celle qui régit la classification des documents, lettres, notes de travail, esquisses grossières, etc. Dans ce cas-ci, l'analogie consiste à appliquer la politique de classification à tous les genres de renseignements enregistrés, bien que la définition soit axée sur les documents imprimés. Pour ce qui a trait à la bureautique, on pourrait se demander comment appliquer la politique de classification aux brouillons de "documents électroniques" ou aux informations stockées dans le "dossier privé" d'une personne.

La combinaison des politiques de sécurité actuelles du gouvernement, de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels semble devoir entraîner deux catégories principales de classification de l'information, aux fins de leur protection. La première porterait sur le domaine traditionnel de l'information touchant les intérêts de la défense de la nation, où les considérations de coût et de baisse possible de l'efficacité opérationnelle à cause de la restriction de l'accès passent après les niveaux de sécurité qu'il faut assurer aux données. L'autre viserait l'information dont la communication au public risque de nuire aux intérêts des parties concernées (p. ex. le gouvernement, les entreprises et les personnes). C'est ce qu'on pourrait appeler les renseignements "confidentiels". Il s'agit en fait d'une nouvelle catégorie issue des exceptions subjectives en vertu de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels ainsi que de l'avènement du principe juridique de l'équilibre à créer entre le droit d'accès et les préjudices que

causerait la divulgation des informations. L'une des possibilités à explorer dans l'utilisation des systèmes bureautiques dans l'administration fédérale consiste à établir une distinction nette entre les systèmes qui peuvent répondre aux exigences de sécurité rigoureuses pour les informations vitales aux intérêts de la nation et ceux qui peuvent satisfaire aux exigences moins strictes de sécurité des renseignements confidentiels.

V. EXIGENCES DE SÉCURITÉ DES DONNÉES EN BUREAUTIQUE DANS LE SECTEUR PRIVÉ

Le Programme de la bureautique a été créé surtout pour aider les fabricants canadiens à élaborer et à tester en milieu réel diverses configurations de systèmes bureautiques, pour améliorer la position concurrentielle de l'industrie canadienne et la rendre apte "à satisfaire à la demande d'un marché qui est appelé à devenir de plus en plus important, tant au Canada qu'à l'étranger". On s'est toutefois demandé, au cours de l'étude, si le gouvernement fédéral, en général, et les cinq centres des essais en milieu réel, en particulier, pouvaient être considérés comme représentatifs des besoins en bureautique du secteur privé et si les exigences de sécurité des données du bureau électronique de l'administration fédérale s'appliquent au secteur privé.

Il convient de signaler tout de suite qu'il existe deux différences essentielles entre le secteur public fédéral et le secteur privé, en ce qui concerne les exigences de sécurité des données.

Premièrement, au gouvernement fédéral, il existe effectivement des renseignements et des systèmes de soutien automatisés correspondants, qu'il faut protéger contre la divulgation non autorisée, "indépendamment du coût", parce que des intérêts vitaux de la nation sont en jeu. Cependant, il s'agit là d'un marché secondaire très spécialisé des technologies de l'ordinateur, des communications et de l'information, en marge du marché général de l'équipement bureautique. Bien que la demande existe pour cette technologie, dans le secteur public et dans le secteur privé, nous ne pouvions dans le présent rapport qu'aborder ce sujet dans ses grandes lignes, comme nous l'avons fait.

Deuxièmement, les organismes fédéraux sont tenus de se conformer aux lois qui imposent le respect de certaines règles sur la consultation, l'utilisation, la communication et la protection de catégories particulières d'informations entregistrées, c'est-à-dire à la Loi sur l'accès à l'information et à la Loi sur la protection des renseignements personnels. Quant à savoir si cette exigence au gouvernement fédéral

s'applique au secteur privé, il existe dans de nombreux pays européens des lois régissant l'information qui s'appliquent au secteur privé, soit des lois qui protègent la vie privée. En outre, le Canada a maintenant officiellement accepté d'adhérer aux Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE. Ces lignes directrices prévoient l'encouragement de tous les organismes des secteurs public et privé à adopter de leur plein gré le Code de protection de la vie privé de l'OCDE, c'est-à-dire le droit à la protection des renseignements personnels détenus par l'organisme. Un certain nombre d'entreprises canadiennes ont en effet déjà intégré ce droit à leurs politiques. Parmi les exemples dignes de mention, il convient de citer IBM, diverses sociétés d'assurances et, récemment, la Banque royale. On estime en outre que beaucoup plus d'une centaine de sociétés multinationales américaines ont déjà mis en application le Code de protection de la vie privée de l'OCDE, ou sont en voie de le faire. À noter que les exigences de la protection de la vie privée sont en réalité un sous-ensemble des bonnes méthodes de gestion de l'information en général (c'est-à-dire garantissant des renseignements opportuns, exacts et pertinents) et des procédures de sécurité des données, en particulier (c'est-à-dire assurant la protection des renseignements personnels contre l'accès et la communication non autorisés). Par conséquent, tout système bureautique du gouvernement fédéral qui peut répondre aux exigences de sécurité des données de la Loi sur la protection des renseignements personnels ne manquera pas d'avoir la préférence sur le marché, non seulement au Canada, mais aussi à l'étranger. En résumé, à la lumière des tendances qui se dessinent dans le contexte des politiques de l'information, il y a lieu de dire qu'un produit qui assure la protection des renseignements personnels donnerait à son fabricant au Canada un net avantage sur la concurrence, étant donné que peu de produits ou sinon aucun en font autant à l'heure actuelle.

D'autre similitudes peuvent être soulignées entre les exigences de sécurité des données des établissements fédéraux et celles du secteur privé. À ce propos, l'objet de la bureautique n'est pas seulement d'accroître

la productivité, mais également d'améliorer la prise de décision. Pour les cadres supérieurs d'un organisme, le potentiel de la bureautique revêt une importance particulière, puisque la bureautique permet de consulter facilement les informations clés, et ce à tout moment, indépendamment de l'endroit où l'on se trouve, réduisant ainsi au minimum les retards et les pertes de temps en transmission, etc. Dans le présent contexte, on peut soutenir qu'il existe une analogie entre les exigences fonctionnelles des secteurs public et privé ainsi qu'entre les rapports des gestionnaires supérieurs d'un ministère avec leur ministre et ceux des cadres supérieurs avec le président d'une entreprise.

Par exemple, l'élaboration d'une importante politique gouvernementale dans un délai déterminé et en vue d'une date de lancement critique exige qu'un nombre restreint de personnes clés puissent, depuis plusieurs endroits à Ottawa et peut-être au Canada, communiquer des renseignements sous forme de projets de documents, opinions, etc., tout en garantissant à ces informations certains degrés de sécurité. Il n'en est pas autrement dans une entreprise, où l'on traite parfois d'une affaire importante, d'un changement dans la direction de l'entreprise, d'un rachat, etc. Très souvent, des mots de passe sont employés, différents groupes de personnes sont concernés (et par conséquent, tous les autres intervenants doivent être exclus de l'accès à l'information), la documentation (sur papier et électronique) doit être tenue séparément, etc. Bref, la Loi sur l'accès à l'information ainsi que la séparation des documents d'un ministère de ceux du Cabinet du ministre, la distinction entre les documents ordinaires et les documents confidentiels du Cabinet, etc. sont autant d'exigences relatives à la sécurité des données qui sont aussi nécessaires au secteur privé, surtout lorsque les cadres supérieurs désirent compter en toute confiance sur un système bureautique. En deux mots, ces exigences consistent à pouvoir assurer différents degrés de protection à des unités d'information figurant dans un "classeur électronique" et accessibles aux seuls groupes (qui varient souvent) de personnes qui en ont besoin dans l'exercice de leurs fonctions.

Sur le plan quotidien ou opérationnel, au gouvernement fédéral, il existe également des similitudes entre les dispositions de la Loi sur l'accès à l'information et les besoins du secteur privé. Parmi les renseignements confidentiels à protéger, on peut citer les secrets de fabrication, les renseignements sur la création de produits, les données financières, y compris la planification budgétaire, les enquêtes (internes), les stratégies et les tactiques de lancement d'une politique, d'un produit ou de services nouveaux, la réorganisation de l'organisme, la planification des carrières, etc. Ce qui distingue ici la protection des renseignements confidentiels du gouvernement fédéral de celle du secteur privé, c'est que, dans le premier cas, les dispositions découlent des lois ou des politiques globales du gouvernement, alors que, dans le second, leur mise en oeuvre dépend de l'analyse des coûts et des risques à prendre. Par conséquent, les systèmes bureautiques conformes à la Loi sur l'accès à l'information et à la Loi sur la protection des renseignements personnels, aux politiques du gouvernement régissant les documents ministériels, les renseignements confidentiels du Cabinet, la protection des informations gouvernementales générales, etc., et comportant des fonctions de sécurité des données, seront sans doute plus commercialisables dans le secteur privé. Cela est d'autant plus vrai que l'ajout après coup de telles fonctions à un système existant est très coûteux, parfois au point de ne plus être rentable pour l'entreprise.

Les énoncés qui précèdent devraient être considérés comme des remarques préliminaires uniquement, puisque l'examen approfondi des besoins du secteur privé en matière de sécurité des données était au départ loin de faire l'objet de la présente étude. Toutefois, il est vrai qu'à l'exception des considérations de sécurité nationale, le gouvernement fédéral a actuellement des obligations de protection des données plus strictes que celles du secteur privé.

Cependant, pour certaines de ces dispositions (p. ex. la protection des renseignements personnels), on constate une tendance internationale à étendre les exigences au secteur privé, alors que pour d'autres, les exigences fonctionnelles des organismes fédéraux sont très semblables à

celles du secteur privé. Si les essais en milieu réel du Programme de la bureautique doivent servir de banc d'essai à l'élaboration de produits bureautiques pour répondre aux besoins du marché, l'inclusion des considérations de sécurité des données dans ce processus devrait accroître la valeur et la possibilité de commercialiser de tels produits sur le marché canadien et à l'étranger.

VI. CONCLUSIONS ET RECOMMANDATIONS

Les essais actuels de bureautique en milieu réel entrepris en vertu du Programme de la bureautique sont axés sur l'élaboration et l'intégration des équipements informatiques et des télécommunications ainsi que du logiciel connexe. Par conséquent, dans ces essais, on a cherché surtout à assurer la communication entre les différentes composantes et à rendre exploitables les logiciels correspondants. Les objets secondaires des essais en milieu réel sont l'acceptation par les utilisateurs des postes de travail multifonctions dans leurs bureaux ou autres lieux de travail, ainsi que l'étude des questions et des préoccupations reliées à l'ergonomie et aux autres facteurs sociaux. Il n'est donc pas surprenant que les considérations de gestion de l'information, en général, et de sécurité des données, en particulier, n'aient pas été la principale préoccupation lors du lancement des essais.

Il semble bien qu'on se soit intéressé à la sécurité des données dans certains des essais en milieu réel, quoique, dans l'ensemble, il semble qu'on ait été peu conscient du vaste éventail de questions et de préoccupations concernant la sécurité des données, surtout de ce qui constitue des informations confidentielles, par opposition aux informations qui touchent directement la sécurité nationale. Il a été décidé, dès le début de certains essais, que les systèmes bureautiques ne serviraient pas, durant leur rodage, à manipuler des informations confidentielles. Toutefois, les responsables des essais n'ont pas reconnu que, passé ce stade, ils devront tenir compte de la sécurité des données lorsqu'ils décideront si les systèmes bureautiques seront utilisés en permanence, et, le cas échéant, de quelle façon. Il est vrai qu'on n'a pas décidé encore comment et où les essais de bureautique en milieu réel devraient être développés ou mis en place pour être exploités en permanence, mais les intéressés semblent favorables à l'étude des considérations de sécurité des données.

Le contenu informationnel des essais en milieu réel semble être centré sur les secteurs administratifs, plutôt que sur les domaines opérationnels et relatifs aux politiques gouvernementales, c'est-à-dire sur les cheminements des informations relatives au personnel ainsi que sur les données et messages financiers et administratifs. Exception à noter, celle du MDC, où les essais portent sur le secteur des politiques et la correspondance ministérielle, aussi bien que sur les cheminements des documents à l'arrivée et au départ du Cabinet du ministre. Ce sont là les domaines types susceptibles de causer des inquiétudes au sujet de la sécurité des données.

Outre certaines questions de protection des renseignements personnels, les usagers sont dans l'ensemble peu conscients de la nécessité de protéger les données, en général, et de l'application pratique de cette sécurité aux systèmes bureautiques, en particulier. On convient généralement que l'une des questions clés, sinon la plus importante, consiste à informer et éduquer l'usager en matière de sécurité des données. Plus précisément, c'est dans le domaine des renseignements qui ne touchent pas la sécurité nationale et dans celui de la protection à assurer aux informations confidentielles que les malentendus ou l'inconsicience constituent le plus grand obstacle. On a signalé en outre que, lorsque les usagers se familiarisent avec certaines fonctions d'un système et l'utilisent sans difficulté (p. ex. le traitement de textes), ils oublient très vite qu'un tel système n'était pas destiné au traitement ou à la communication de renseignements confidentiels et n'avait pas été conçu dans cette perspective. Certains ont également fait remarquer que, si les usagers actuels des systèmes de bureautique sont peu expérimentés, la vague suivante d'employés comptera de nombreux experts dans tous les secteurs de l'administration, d'où les possibilités croissantes de mauvais usage des renseignements et la nécessité d'intégrer des mesures de sécurité.

On semble s'accorder pour reconnaître que la bureautique est une technologie d'intégration. En même temps, l'incertitude règne quant à l'analogie des questions de sécurité des données en bureautique et de celles du traitement des données, de l'informatique et des communications ou même des documents sur papier. Selon certains, les éléments de sécurité de chacune de ces technologies pourraient s'appliquer à la bureautique, mais cette dernière, à cause de la facilité d'utilisation de ses fonctions de transmission (et de sa portabilité), suscite de nombreuses inquiétudes. On a signalé que la protection de la confidentialité des renseignements confidentiels en bureautique était bien plus qu'une simple question technique. Tout aussi importante est la nécessité d'élaborer, pour l'utilisation quotidienne des systèmes bureautiques, des procédures d'exploitation pratiques et pragmatiques qui tiennent compte non seulement des fonctions techniques de sécurité de ces systèmes, mais également de la manipulation des disquettes et des imprimés, du vidage de la mémoire, de la manipulation des mots de passe, du chiffrement, etc.

Les experts techniques et opérationnels des technologies informatiques et des communications conviennent tous que, si l'on ne tient pas compte des fonctions appropriées de sécurité des données dès les premières étapes de la conception de systèmes bureautiques et de l'élaboration des caractéristiques fonctionnelles, il est en général bien plus coûteux d'ajouter de telles fonctions par la suite. L'essai en milieu réel au ministère des Communications comprend l'utilisation de terminaux intelligents portables ou de micro-ordinateurs. Cette utilisation suscite de nouvelles inquiétudes au sujet de la sécurité des données et doit se faire sous réserve de l'examen des risques additionnels encourus.

Au cours des trois dernières décennies, le gouvernement fédéral a adopté une politique de sécurité en vue de protéger les renseignements touchant la sécurité nationale contre toute divulgation non autorisée et a acquis une vaste expérience dans ce domaine. Bien que l'on s'accorde à dire que la politique de sécurité de 1956 est périmée et doit être remaniée en fonction des technologies de l'information et des nouvelles lois sur l'information, un grand nombre des principes exprimés dans cette

politique s'appliquent toujours. De même, le gouvernement fédéral a élaboré des politiques sur l'accès et l'utilisation des informations, sur l'utilisation des diverses technologies de l'information ainsi que sur la gestion au jour le jour des informations enregistrées. Bon nombre de ces politiques contiennent des éléments qui témoignent des préoccupations relatives à la sécurité. La bureautique englobe tous les aspects des technologies de l'information et de la gestion de l'information, y compris la sécurité.

Le gouvernement fédéral a effectivement adopté des critères et des normes de sécurité des données, auxquels il faut se conformer lorsqu'on utilise le matériel informatique et de transmission pour manipuler des informations confidentielles reliées à l'intérêt national, mais on ne dispose actuellement d'aucun critère précis, pratique et complet pour la manipulation des renseignements confidentiels (ne touchant pas la sécurité nationale) dans divers contextes de traitement électronique des données. Il existe un besoin urgent de tels critères. L'un des objectifs inhérents à la bureautique étant d'accroître l'efficacité de la prise de décisions dans tous les secteurs de l'organisme, il faut être en mesure d'intégrer les informations confidentielles aux systèmes bureautiques. Pour que l'administration fédérale puisse utiliser ces derniers dans des applications aussi diverses que possible, les systèmes et les procédures correspondantes doivent pouvoir satisfaire aux exigences juridiques et administratives fédérales de la politique de l'information sur la communication et l'usage des informations.

Il ne fait aucun doute que les politiques administratives actuelles et nouvelles du gouvernement fédéral concernant l'utilisation des diverses technologies de l'information et la gestion de l'information, y compris celles qui résultent des dispositions de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, s'appliquent également aux informations en bureautique. Cependant, étant donné que la bureautique est une nouvelle technologie d'intégration, on ressent le besoin d'un projet pilote qui vise l'application à cette technologie des nouvelles politiques de gestion de l'information du

gouvernement. Par exemple, l'un des instruments utiles à élaborer consiste en une matrice des types d'informations dont la divulgation est exclue en vertu de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, précisant si l'exclusion est obligatoire ou discrétionnaire, s'il faut appliquer le critère objectif ou subjectif, si la consultation d'autres personnes est nécessaire, etc.; de même, une telle matrice devrait être traduite en caractéristiques obligatoires des systèmes de bureautique à l'usage du gouvernement.

On constate le besoin d'élaborer une série concrète de lignes directrices, de procédures et de méthodes qui garantiraient la conformité de l'utilisation des nouvelles technologies de l'information au gouvernement fédéral avec les dispositions des lois en vigueur et avec les nouvelles politiques de l'information, surtout en ce qui concerne la sécurité des informations confidentielles. L'élaboration d'un tel ensemble de lignes directrices, procédures et méthodes pour les systèmes bureautiques sur les informations confidentielles qui ne sont pas reliées à l'intérêt national constituerait une façon d'expérimenter l'application, intégrée aux systèmes bureautiques, de la politique, des directives, des normes et des lignes directrices du gouvernement régissant le traitement et la transmission des données.

Le ministère des Communications est à l'avant-garde de l'élaboration de systèmes bureautiques. De même, l'essai de la bureautique en milieu réel dans ce ministère comporte l'usage de micro-ordinateurs portables, alors que le domaine d'application est le secteur des politiques et du Cabinet du ministre, c'est-à-dire un secteur où l'on manipule des informations confidentielles. **Pour ces raisons, et à cause du rôle du Ministère dans les domaines de la technologie de pointe en informatique et en communications, y compris la sécurité des communications, il y aurait lieu, pour le MDC, conjointement avec d'autres organismes compétents du gouvernement et d'entreprises représentant le secteur privé, de lancer un projet pilote qui traiterait de façon pratique des préoccupations que suscitent les systèmes bureautiques au sujet de la sécurité des données.**

Les avantages de la bureautisation d'un organisme consistent dans l'accroissement de la productivité et de l'efficacité du processus de prise de décision. Si la bureautique, en tant qu'instrument de productivité pour la manipulation des flux d'informations courants, est d'une rentabilité restreinte, son adoption pour la prise des décisions profite bien plus à l'organisme. Toutefois, pour qu'un système bureautique soit un mécanisme de soutien au processus de prise de décisions, il doit pouvoir manipuler des informations confidentielles et comporter des fonctions qui aident à respecter les obligations en matière de sécurité des données.

Par conséquent, la taille du marché et le rythme de pénétration de ce marché par les fabricants canadiens de matériel bureautique sont directement reliés au degré d'aptitude des systèmes canadiens à manipuler les informations confidentielles. Il en est ainsi surtout du marché du secteur public au Canada et aux États-Unis, qui doit se conformer aux exigences des différentes lois sur l'information.

Pour que les fournisseurs canadiens de systèmes bureautiques aient accès aux plus vastes marchés possibles dans le secteur public fédéral, leurs systèmes doivent pouvoir satisfaire aux exigences de sécurité des données du gouvernement fédéral, y compris celles qui découlent de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels. En outre, comme de nombreuses dispositions des lois fédérales sur l'information sont analogues aux besoins du secteur privé et que ce dernier tend à adopter le droit à la protection des renseignements personnels, il est indispensable que les fournisseurs canadiens en prennent conscience aussitôt que possible.

Par conséquent, il faut attribuer une forte priorité à la préparation, à l'intention des fournisseurs canadiens de systèmes bureautiques, d'un document qui traduise en termes clairs et simples les dispositions de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels ainsi que les préoccupations du gouvernement fédéral en matière de sécurité des données, afin que les fournisseurs

intègrent les fonctions correspondantes dans les produits qu'ils mettent sur le marché. Un tel document devrait également faire le lien entre les exigences actuelles du gouvernement fédéral en matière de sécurité des données et celles du marché au Canada et à l'étranger.

Le présent document ne prétend pas offrir une étude intégrale des questions et préoccupations relatives à la sécurité, à la confidentialité et à la protection des renseignements personnels suscitées par la bureautisation du gouvernement fédéral. Une telle étude exigerait bien plus de temps et couvrirait un champ beaucoup trop vaste. Ce rapport représente plutôt un aperçu préliminaire des sujets de préoccupation. Néanmoins, lorsque les essais de bureautique en milieu réel auront atteint leurs objectifs techniques et qu'on aura appris à régler les principaux problèmes ergonomiques, il est clair qu'il faudra envisager les questions reliées au contenu informationnel et à la sécurité des données.

VII. POSTFACE

Depuis la production du rapport de 1984 sur la sécurité des données, il s'est produit un certain nombre d'événements liés aux questions de sécurité, de confidentialité et de protection des renseignements personnels.

Premièrement, le 15 décembre 1985, une série de modifications au Code criminel sont entrées en vigueur. Deux d'entre elles avaient trait aux fraudes informatiques et à l'abus des données. Avec les articles concernant les fraudes en matière de télécommunication, ces deux modifications semblent offrir une protection adéquate contre l'utilisation non autorisée des technologies des domaines de l'informatique, des communications et de la bureautique de même que des logiciels et des données et corriger la situation. Une étude détaillée de ces nouvelles modifications est faite dans une publication mise à la disposition des participants au Carrefour international de l'information électronique et intitulée Questions de droit que posent les systèmes informatiques intégrés : Aperçu des considérations pratiques et des récents développements.

Deuxièmement, les études sur la sécurité des données faites en 1984 ont mis en lumière le fait que les lois concernant l'information étaient une des raisons principales expliquant les préoccupations et les besoins en matière de protection des données. On s'est également rendu compte que les liens entre les lois concernant l'information et la gestion des données (notamment les aspects concernant la sécurité, la confidentialité, la protection des données) n'étaient pas bien compris. En conséquence, on a entrepris une série d'études visant à corriger les anomalies constatées dans le rapport sur les Questions d'ordre légal mentionnées précédemment. En plus du Code criminel, le rapport examine également les préoccupations en matière de sécurité, de confidentialité et de protection des données résultant de la Loi sur la preuve au Canada (par exemple, l'admissibilité en preuve des états produits par ordinateur, l'authentification, etc.) la Loi sur l'accès à l'information et la loi sur la protection des renseignements personnels, les droits d'auteurs et les exigences relatives à la conservation des dossiers (par exemple, devrait-on y apporter des modifications pour permettre la conservation des états informatiques)?

Dans ce contexte, notons que le comité parlementaire qui a étudié les trois premières années d'application de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels a recommandé au gouvernement fédéral, dans son rapport de 1987, d'incorporer dans la Loi sur la protection des renseignements personnels certaines mesures de protection des données.

Le comité a spécifiquement recommandé "... d'adopter des mesures de sécurité administratives, techniques et physiques appropriées pour assurer la sécurité et la confidentialité des dossiers et pour les protéger contre toute menace ou danger éventuel à leur sécurité ou à leur intégrité..." (recommandation 5.25, p. 28). La loi de la province de Québec sur la protection des renseignements personnels contient déjà des exigences de ce genre.

La troisième activité principale qui a suivi le rapport de 1984 sur la protection des données a été la mission confiée par le ministère des Communications de faire des études en vue de déterminer les besoins des utilisateurs du secteur privé en matière de sécurité, de confidentialité et de protection des données dans les systèmes bureautiques intégrés et dans l'échange d'informations. Entreprise par la société Stevenson Kellogg Ernest et Whinney, consultants en gestion, appuyée par Thorne Ernest et Whinney, comptables agréés et Infoman Inc., consultants en gestion et en politiques en matière d'information, l'étude visait à :

- déterminer, par l'examen d'ouvrages, d'études et de travaux de groupes de recherches, les besoins du secteur privé (c.-à-d. les organisations non gouvernementales) en matière de confidentialité, de sécurité et de protection des renseignements dans les systèmes bureautiques;

- déterminer si le passage du papier aux documents "électroniques" dans les systèmes bureautiques entraîne des problèmes nouveaux ou différents et un ensemble de besoins différent en matière de système;

- établir une liste des besoins des utilisateurs qui pourrait servir aux fournisseurs et aux organisations cherchant à élaborer et à exploiter les produits; et

- faire en sorte que les résultats de l'étude fassent partie de la contribution canadienne à l'élaboration de normes en matière de protection par l'International Standards Organization (ISO).

Ces études devraient être complétées à l'automne de 1987.

Quatrièmement, notons que le Centre canadien de recherches sur l'informatisation du travail (CCRIT) et les Archives publiques du Canada parrainent un projet qui donnera lieu à l'élaboration de "spécifications fonctionnelles pour la gestion de documents électroniques dans les systèmes bureautiques (ISO)". Un groupe de travail composé de représentants et d'experts d'organismes fédéraux importants et de l'industrie prévoit produire un ensemble de projets de normes à l'été de 1987. Ce qui est intéressant, pour ce qui a trait à la protection des données, c'est qu'un nombre important de ces spécifications fonctionnelles auront trait à des questions d'accès et de confidentialité, de classification, de protection des renseignements, de protection et de conservation de données de grande importance, d'accès et de contrôle d'utilisation, etc.

Enfin, depuis 1984, le gouvernement fédéral a entrepris une importante révision de sa politique en matière de sécurité. Celle-ci a donné lieu à la publication, le 18 juin 1986, par le Secrétariat du Conseil du Trésor, d'une nouvelle "politique du gouvernement canadien en matière de sécurité" et d'un ensemble de "lignes de conduite concernant la mise en place de la politique en matière de sécurité" le 11 août 1986.

La nouvelle politique en matière de sécurité comporte un certain nombre de caractéristiques qu'il convient de mettre en évidence; on a notamment :

- adopté une approche libérée de la technologie pour ce qui est de la protection de l'information et on prévoit un cadre et des normes de gestion généraux pour ce qui est de la protection des données au gouvernement; et,

- établi deux types principaux de classification de sécurité; le premier ensemble concerne l'information d'intérêt national. Voici les différentes catégories retenues :

TRÈS SECRET - vise à prévenir un tort particulièrement grave à l'intérêt national,

SECRET - vise à prévenir un tort grave à l'intérêt national,

CONFIDENTIEL - vise à prévenir un tort à l'intérêt national.

On a abandonné la cote DIFFUSION RESTREINTE qui ne peut désormais être attribuée qu'au matériel reçu de l'OTAN et de l'OCDE et faisant partie de cette catégorie.

L'aspect le plus important de la nouvelle politique en matière de sécurité, c'est qu'elle vise à réduire le nombre de documents qu'il faut classer. Pour ce faire, on a établi une nouvelle catégorie de protection de l'information "sensible" (conformément à ce qui a été suggéré dans le rapport de 1984 concernant la protection des données). La nouvelle politique comprend une nouvelle catégorie, soit "l'information PROTÉGÉE", c'est-à-dire celle qu'il faut protéger davantage, mais qui n'est pas d'intérêt national. Par exemple, l'information à laquelle on ne peut accéder en vertu de certaines dispositions de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels (par exemple, des données personnelles, celles qui ont trait à un tiers, les données relatives à l'application de la loi et les données d'enquête). Pour protéger ces informations, on en limite l'accès aux personnes qui ont "besoin de savoir".

Il se peut que les exigences en matière de protection des données dans les systèmes bureautiques intégrés, pour ce qui est de l'information "PROTÉGÉE" dans le secteur public, correspondent à celles qu'on impose en général dans le secteur privé.

Il sera également très intéressant de savoir dans quelle mesure la situation canadienne ressemble à celle d'autres pays ou diffère de celle-ci. Les commentaires des participants au CIIEL sur la sécurité des données et sur des questions connexes dans les systèmes informatiques intégrés seront donc des plus appréciés.

RÉFÉRENCES

Voici une brève liste des documents consultés, outre ceux qui sont cités dans le rapport.

1. L'avènement du bureau électronique au Canada, Communications Canada, mai 1982, 40 pages.

2. Un avant-goût de l'avenir: la bureautique à l'administration fédérale, Communications Canada, printemps 1984, 25 pages.

3. Informatique. Normes et méthodes de sécurité à l'usage des ministères et des organismes du gouvernement du Canada, Normes gouvernementales en informatique GES/NGI-14, juin 1980 (en cours de révision).

4. Knoppers, Jake V. Th., Report on Vulnerability Issues, Interdepartmental Task Force on Transborder Data Flows, ministère des Communications, décembre 1982, 102 pages.

5. Knoppers, Jake V. Th., Report on Possible Security/Confidentiality Implications of the Application Areas and Information Content of the OCS Field Trials, par la Division des programmes et des opérations de sécurité, ministère des Communications, mars 1984, 29 pages.

6. Knoppers, Jake V. Th., Report on Key Federal Information Legislation and Information Policies which Impact on Possible Security/Confidentiality Implications in the OCS Program, par la Division des programmes et des opérations de sécurité, ministère des Communications, mars 1984, 47 pages et annexe de 22 pages.

7. Knoppers, Jake V. Th., Security Confidentiality in the Electronic Office: A Preliminary Review of Issues and Concerns in the Federal Government Sector, juin 1984, 38 pages.

8. John McDonald, Rapport provisoire du groupe de travail de gestion de l'information APC/MDC, Archives publiques du Canada, juin 1984, 62 pages et annexes.

9. Une question à deux volets: Comment améliorer le droit d'accès à l'information tout en renforcant les mesures de protection des renseignements personnels, Examen de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels : rapport du comité permanent de la Justice et du Solliciteur général, Ottawa, mars 1984, 150 pages.

10. Politique concernant la sécurité du gouvernement, Circulaire no 1986-26, Secrétariat du Conseil du Trésor, Ottawa, le 18 juin 1986, 22 pages et annexes.

11. Lignes directrices concernant la mise en oeuvre de la politique sur la sécurité, Circulaire no 1986-41, Secrétariat du Conseil du Trésor, Ottawa, le 11 août 1986, 45 pages.

CACC / CCAC
89642

--KNOPPERS, JAKE V. TH.
--Sécurité des données en bureautique: exploration des questions et des préoccupations suscitées par le programme de la bureautique.

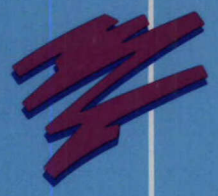
P
91
C655
K583f
1987

DUE DATE

201-6503

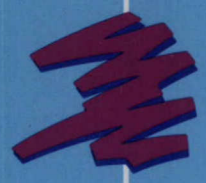
Printed in USA

QUEEN P 91 .C655 K58314 1987
Knoppers, Jake V. Th
Securite des donnees en bure



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