ÉTUDE

*Les courriels : actif informationnel de nos organisations**

Carole Saulnier

Cet article porte sur le courrier électronique comme actif informationnel important de nos organisations. Nous y verrons, après un bref historique du courriel, la façon dont cette application fonctionne et la toile de fond actuelle régissant son emploi dans nos organisations. Mes propos porteront ensuite sur les quatre défis auxquels nous sommes confrontés dans l'utilisation et la gestion du courriel et cerneront quelques pistes de solution. J'ai choisi d'être volontairement un peu technique, en premier lieu parce qu'il me semble très intéressant de nous doter, nous archivistes, d'un vocabulaire nous laissant moins démunis face aux informaticiens ou aux gestionnaires et, en second lieu, parce qu'il me semble qu'une fois comprises certaines notions de base, il est possible de mieux se situer dans les enjeux et rôles qui nous incombent.

HISTORIQUE

On peut remonter l'origine du courriel à la découverte, dans les années 1960, du *timesharing,* c'est-à-dire du fait qu'un ordinateur peut effectuer plusieurs tâches en ce qui nous semble, à nous, être le même temps. À cette époque, un ordinateur était une immense machine (*main frame*) installée dans une salle spécialement conçue pour elle, à laquelle étaient branchés des dizaines ou des centaines de terminaux. Ceci permettait à des chercheurs, utilisant chacun leur terminal, de communiquer entre eux en une forme de « chat » ou « clavardage ».

C'est le 29 octobre 1969[1] que fut faite la première tentative pour faire parler entre eux deux ordinateurs : celui de la University of California at Los Angeles (UCLA) et celui du Stanford Research Institute. Internet, qui s'appelait alors ARPANET (Advanced Research Project Agency), n'était constitué que de quatre ordinateurs branchés ensemble : celui de la UCLA, celui du Stanford Research Institute, et ceux de la University

* Ce texte est une version mise à jour d'une conférence donnée par l'auteure dans le cadre du 33e Congrès de l'Association des archivistes du Québec tenu à Sainte-Adèle en 2004.

of California at Santa Barbara et de la University of Utah. La plus grosse composante était constituée d'un miniordinateur Honeywell de 12 Ko seulement de mémoire[2] !

C'est cependant en 1971[3] que Ray Tomlinson a développé la première véritable application de courriel pour l'Arpanet. Elle consistait en un premier programme pour envoyer des courriels, appelé SNDMSG (*send message*) et un autre appelé READMAIL pour lire, sauvegarder ou détruire les messages, les trier par en-tête, sujets et date dans les boîtes de réception. Son modèle est devenu le modèle de base qui est encore en usage maintenant.

L'utilisation de cette fonctionnalité, à cette époque, n'était offerte qu'à quelques scientifiques. Elle fonctionnait au moyen du protocole normalisé FTP (File Transfer Protocol). On utilise encore le FTP pour sa très grande capacité de télédéchargement. Par exemple, lorsque des fichiers sont trop volumineux pour l'application de courriel utilisée, c'est encore aujourd'hui la méthode employée. Par contre, le FTP fonctionne de façon à copier le message qui doit être envoyé à chaque destinataire et il l'envoie effectivement séparément à chacune des personnes. Cela en fait donc une application plus lourde qui occasionne plus de trafic.

Au milieu des années 1970, soixante-quatre ordinateurs seulement étaient connectés entre eux. En 1975 c'est Unix qui entre dans le jeu et développe des applications semblables pour ses machines. En 1977, une première initiative visant à rendre cohérents les différents formats en usage pour le courriel produit un premier standard (RFC733). L'année suivante, l'Université du Delaware réalise un projet, commandé par le Department of Defense (DOD), qui vise à alimenter en courriels des ordinateurs non reliés à Arpanet, utilisant pour ce faire, les lignes téléphoniques.

Dans les années 1980, on développe le SMTP (Simple Mail Transfert Protocol, norme RFC822) de façon à être plus efficace. En effet ce protocole, encore en usage pour l'envoi des messages, est constitué de dix commandes très simples et il permet, au contraire du FTP, l'envoi d'un message unique à chaque domaine où il y a plusieurs correspondants et où, là seulement, le message est copié pour chacun des correspondants, ce qui est moins lourd et plus rapide pour le système. C'est donc en 1982 que ce standard Internet, qui décrit entre autres la syntaxe des noms de domaines (comme par exemple « ulaval.ca », « gouv.qc.ca » ou « hotmail.com »), voit le jour, standard sur lequel sont basés nos serveurs de courrier encore maintenant.

C'est véritablement en 1988 que Vinton Cerf, avec le programme TCP/IP (Transmission Control Program / Internet Protocol), déploie véritablement le protocole de réseau le plus utilisé au monde et donne l'essor définitif à l'échange de courriel par Internet. Enfin, en 1993, AOL et Delphi, deux très importants fournisseurs de services internet propriétaires, se connectent ou « se convertissent », permettant ainsi de faire accéder le courriel comme standard global.

Comment cela fonctionne véritablement

Comme nous avons pu le constater, un système de courrier électronique est en fait constitué de deux parties : une première pour l'expédition du message et une seconde, le logiciel-client, pour lire, classer, trier ou détruire le message.

La partie expédition est en fait un serveur qui utilise le protocole SMTP (RFC822) et qui, lorsqu'un message est envoyé, consulte d'abord sa base de données sur les noms de domaine (ce qu'on appelle le « record MX ») afin de voir si les destinataires du message ne font pas partie de son propre domaine. En cas contraire, il contacte l'autre serveur afin de vérifier si l'adresse du destinataire est valide et, si oui, transfère effectivement le message.

Il y a trois grands types de serveurs pour ce faire : Unix, qui utilise entre autres Sendmail, Postfix et plusieurs autres ; Exchange, pour les produits Microsoft, qui utilise IIS ; et, bien entendu, Lotus Notes de IBM, dont l'usage a débuté dans les années 1970. Dans un article sur les serveurs de courriels qui sont en fait des *groupware* [que je traduis ici par « groupiciels »], c'est-à-dire des serveurs qui fournissent, en plus du courriel, des fonctionnalités d'agenda de groupes, de partage de documents, de bottin, etc., la revue *PC Magazine*[4] comparait récemment (en 2004) les coûts de ces services pour des entreprises de cinquante à mille deux cent cinquante employés.

Voici le tableau comparatif :

Compagnie	50 postes	250 postes	1250 postes
Novell	6,500 $	32,500 $	162,500 $
Lotus Domino	5,950 $	29,750 $	145,000 $
Microsoft Exchange	4,049 $	17,449 $	84,499 $
MailSite SE	2,095 $	6,993 $	26,563 $
CommuniGate Pro (de Stalker)	499 $	1,500$	3,497 $

Pour lire les courriels, les principaux logiciels clients sont Outlook de Microsoft, Eudora de Qualcomm, Notes pour Lotus de IBM et ceux intégrés aux principaux navigateurs comme Netscape, Internet Explorer, Mozilla, etc. Il en existe également plusieurs autres comme : IncrediMail, Pegasus, en distribution libre (shareware) Bloomba, PocoMail, ou encore les applications Web comme Hotmail, Yahoo, etc.

Mais, peu importe les logiciels clients ou les interfaces Web, tous répondent à des protocoles également normés. Ces protocoles sont nommés POP3, IMAP ou MAPI.

- POP3 (Post Office Protocol 3), la connection client la plus répandue, utilise douze commandes fort simples du type « list », « retr » (*retrive*), « del » (détruire le message) ou « rset » (*remove messages deleted*). Ce protocole permet à chaque logiciel client, partout dans le monde, de se connecter à Internet et d'utiliser, en autant que la personne possède un compte et un mot de passe valides, les fonctions habituelles de lecture et d'envoi.

  La particularité des logiciels utilisant le POP3 est qu'ils vont chercher sur le serveur les courriels et, en les téléchargeant sur le poste, en libèrent le serveur. On comprendra que cette fonctionnalité est très appréciée par les informaticiens et administrateurs des serveurs, surtout quand ils ont des milliers d'abonnés.
- IMAP (Internet Message Application Protocol) est un peu moins commun mais plus complet que POP3. Sa particularité est qu'il laisse les messages sur le serveur. On peut donc les lire n'importe où dans le monde et y revenir autant à la maison qu'au bureau ou en voyage.

- Pour Microsoft, avec les serveurs Exchange, c'est le protocole MAPI (Messaging Application Programming Interface) qui ressemble, dans ses fonctionnalités, à IMAP.

TOILE DE FOND ACTUELLE

À peu près tout le monde, à l'heure actuelle, conçoit le courriel comme une partie essentielle de l'infrastructure de communication des organisations. En effet, les mentalités ont évolué sur ce point, amenant les employés, même les plus réfractaires au départ, à utiliser et même sur-utiliser ce moyen de communication. Les abus de toutes sortes (blagues envoyées à un réseau de connaissances, offres d'achat du berceau du petit dernier, petits films drôles ou salaces, recettes de cuisine ou simplement réponses intempestives à des listes regroupant des centaines de personnes, etc.) ont contribué à engorger les réseaux et ont amené plusieurs organisations soit à interdire carrément, sous diverses peines, l'emploi du courriel à des fins personnelles, soit à en encadrer sérieusement la pratique dans des politiques, codes d'éthique et procédures. Devant certains cas très médiatisés, dont certains, en particulier aux États-Unis, ont fait jurisprudence et dans le contexte de l'application de la *Loi concernant le cadre juridique des technologies de l'information*, plusieurs organismes ont jugé intéressant de produire de tels outils[5].

On peut donc dire que, depuis la fin des années 1990, la plupart des grandes entreprises ont carrément intégré le courriel dans leurs processus d'affaires courants comme l'échange de contrats et leurs négociations, les campagnes de marketing, les listes de clients potentiels, échangées ou créées par courriel et les commandes et confirmations des commandes. Le courriel est devenu le processus privilégié pour mener des affaires – on parle même de 90% des compagnies qui l'utilisent comme tel. Et on sait qu'aux États-Unis seulement, 1.7 millions de nouvelles adresses courriel s'ajoutent à chaque année[6] !

Ce changement dans les mentalités a cependant un revers qui coûte cher aux organisations. En effet en 2003, selon Postini[7], un hôte californien dont les serveurs accueillent de 150 à 200 millions de courriels par jour, les « spam » (ou messages non sollicités ou indésirables) en comptent pour la moitié (Postini Integrated Message Management). D'où également le danger de dissémination des virus. Le ratio *messages / messages infectés de virus* a augmenté de 85% d'après MessagesLab une autre firme de New York. Les organisations n'ont évidemment pas besoin de cela. Ce raz-de-marée de pourriels fait en sorte également qu'il devient très possible de « perdre » des courriels importants, soit parce que les filtres mis en place par les employés sont trop rigoureux, soit parce que le titre du message n'est pas assez explicite. Des études menées par le Gartner Group, une multinationale de conseil et de recherche basée au Connecticut, arrivaient à la conclusion, en 2001, que chaque employé utilisateur de courriels perdait 49 minutes par jour à seulement gérer ses courriels – non à les lire ou à y répondre, mais bien seulement à les gérer[8].

Selon International Data Corporation (IDC) une multinationale qui se spécialise dans l'avenir de l'industrie des technologies de l'information, le nombre de courriels envoyés chaque jour a augmenté de 9.7 milliards qu'il était en 2000, à 35 milliards en

2005[9] (Mayer 2003, 3). Bien qu'en décembre 2003 le congrès américain ait passé une loi visant non à enrayer mais bien à contrôler les « spams », nous sommes en droit de nous attendre à peu d'effets de cette législation ; et ceci même si quatre « spammers » de la banlieue de Détroit ont été mis en accusation en 2004[10]. En effet, pour changer cet état de fait, il faudrait changer complètement les mentalités et les manières de commercer[11].

Toutes ces difficultés dans l'utilisation du courrier électronique font en sorte que de plus en plus de personnes ou d'organismes aimeraient délaisser le courriel. Ainsi, General Motor (GM) qui emploie 340,000 personnes partout dans le monde commence tranquillement à délaisser ce moyen de commmunication et, selon une étude récente de Insight Express (Connecticut), 42% des 500 PME interrogées considèrent laisser tomber le courriel si tous ces spams et pourriels continuent et s'accroissent encore[12].

Vers quoi vont-ils se diriger ? Vers les systèmes de messageries instantannées (du type Messenger) où maintenant sont incorporés les images, les sons et les documents attachés. Cette tendance est confirmée par la firme de recherche IDC qui prétend que plus de 170 millions de personnes possèdent un compte Messenger et que le tiers de ces utilisateurs sont en fait des entreprises qui y trouvent ainsi une façon d'effectuer du « travail en groupe ».

DÉFIS LIÉS À L'UTILISATION ADÉQUATE DU COURRIEL

Tels sont certains des problèmes occasionnés par l'utilisation du courriel. Il devient donc nécessaire de s'interroger sur ce que devrait devenir cette application pour satisfaire véritablement les besoins de nos organisations.

On le sait, la ressource documentaire est vitale pour toute organisation[13]. Elle fait partie de ses stratégies d'existence et sert chez elle quatre objectifs fondamentaux : confirmer les droits des personnes physiques et morales, renseigner sur des connaissances essentielles, appuyer la réflexion et l'analyse et faciliter l'application des décisions. Il s'agit donc d'une ressource essentielle. Or, sous sa forme électronique, elle ne répond pas présentement aux obligations d'accessibilité, de sécurité, de conservation et d'élimination auxquels les organisations sont soumises.

Les conséquences sont de quatre ordres. Les gestionnaires ne peuvent repérer leur information à temps ; les informaticiens ne savent quoi « effacer » pour redonner à leur environnement la performance que les utilisateurs en attendent, les usagers, eux, ne savent quoi détruire, classer ou préserver ; et l'organisation manque à son devoir de se pourvoir d'outils lui permettant de consigner l'information administrative et d'asseoir ses droits.

Ainsi, non seulement la prise de décision devient hasardeuse, l'information critique n'étant pas toujours disponible ou même connue, mais il y a également le risque de se retrouver avec une discontinuité dans les archives institutionnelles et une diminution de la protection des intérêts juridiques, financiers et administratifs des organisations. De plus, la tendance actuelle du mode de gestion, caractérisée par le roulement régulier de la majorité des administrateurs, et la complexification des organisations jointe à la venue de technologies en matière de création, de traitement, de communication et de maintien de l'information, changent singulièrement les façons de faire et viennent accentuer ces problèmes.

Voyons maintenant, regroupés en quatre thèmes, à savoir la sécurité, la valeur de preuve, la gestion et le contrôle des documents produits ou transmis et la préservation, quels sont les défis posés par ce moyen de communication.

Sécurité

La sécurité des courriels fait référence à deux réalités : d'abord la confidentialité des données et ensuite la présence de copies de sauvegarde des courriels.

Un mot seulement sur la *sauvegarde* des courriels. Malgré le fait que de grandes quantités de documents critiques pour les organisations sont créés, maintenus et conservés dans des systèmes de courriel, leurs copies de sauvegarde (*back-up*) sont souvent incomplètes. En effet, un courriel arrivant sur un serveur avec le protocole POP3 et lu dans la même journée ne pourra être copié dans la sauvegarde qui se fait habituellement la nuit. On peut donc présumer que les messages très importants et, conséquemment, urgents la plupart du temps, sont susceptibles d'être les premiers à passer outre ce simple moyen de protection. On ne tiendra donc pas compte de cette fonctionnalité lorsque nous parlerons de la préservation ou de la conservation des courriels.

Dans le même ordre d'idées, on éprouve également certaines des difficultés inverses, dans les systèmes conservant les courriels sur les serveurs (IMAP ou MAPI), qui sont, de détruire véritablement les messages périmés. En effet, ceux-ci sont stockés dans le logiciel ou ailleurs dans des entrepôts virtuels mais le chemin d'accès n'en est pas toujours évident et les sauvegardes nombreuses font que, lorsque le système tombe et est restoré à partir des *back-up*, tous les messages, même ceux effacés, peuvent être rendus disponibles à nouveau. Il ne faut pas oublier non plus qu'un message jeté à la corbeille n'est pas réellement effacé et serait repéré facilement par un moteur de recherche simple, par exemple dans le cadre d'une demande d'accès.

La *confidentialité* pour sa part consiste à rendre l'information inintelligible à toute personne autre que les acteurs de la transaction. Quand on parle de confidentialité il faut sous-entendre automatiquement la cryptographie ou le chiffrement.

De tout temps l'échange de messages secrets entre deux parties a reposé sur l'envoi d'une quelconque « clé » par un messager qui avait toute la confiance des parties. Aux siècles derniers, on utilisait les services d'un messager qui transmettait le message oralement ou sur papier. Mais comme il pouvait être intercepté, torturé et qu'il pouvait parler (!), cela n'était pas considéré comme un moyen très sûr. Une des premières sociétés à pratiquer les messages secrets a été celle des Babyloniens sous Nabuchodonosor. Celui-ci faisait tatouer le message à délivrer sur le crâne rasé d'un messager qui, lorsqu'il atteignait, après plusieurs mois, sa destination, se rasait à nouveau pour délivrer son message[14].

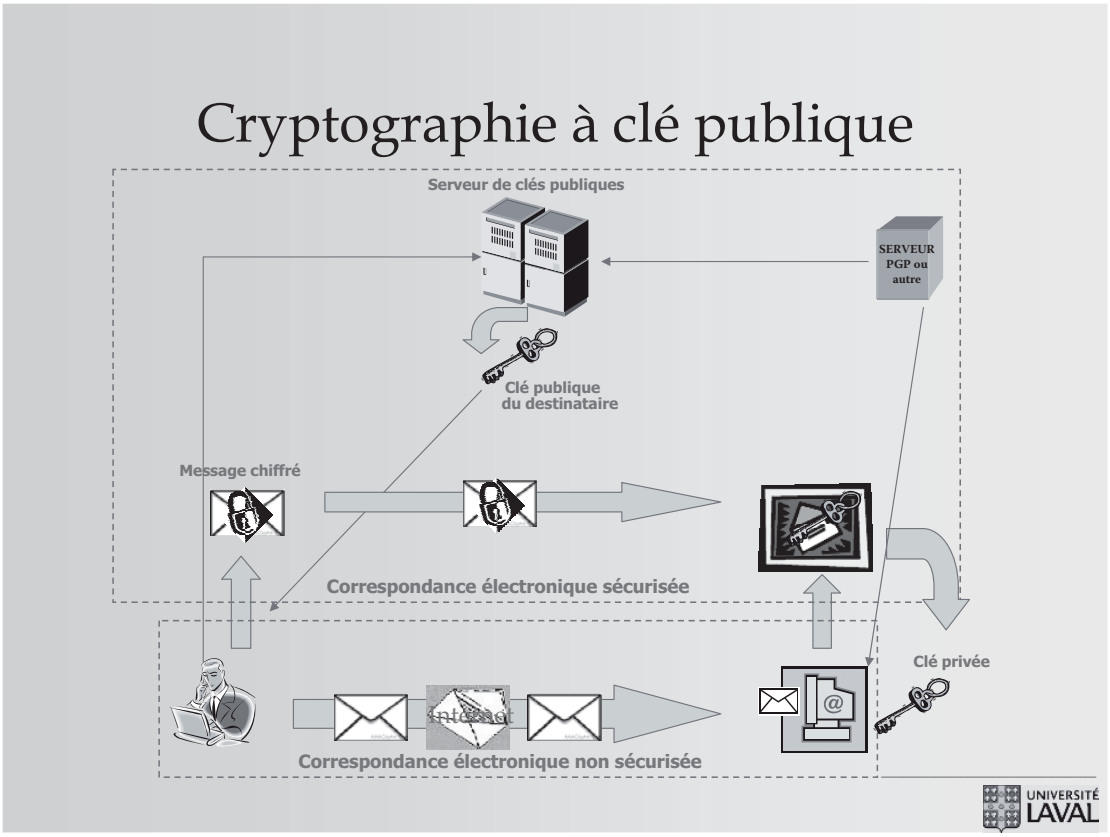
Aujourd'hui, la cryptographie a un intérêt d'autant plus grand que les communications via Internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. De plus, elle sert non seulement à préserver la confidentialité des données, mais aussi à garantir leur *intégrité* et leur *authenticité*.

Les premières expériences de cryptographie dans le domaine électronique se sont concrétisées dans ce qui fut nommé la cryptographie symétrique ou à clé secrète. Elles reposaient sur l'utilisation d'une clé mathématique unique qui sert au chiffrement et au

déchiffrement des données (clés symétriques). Ainsi, pour faire parvenir un message de façon sécurisée, il fallait le chiffrer à l'aide d'une clé (un algorithme) connue uniquement de l'expéditeur. On faisait ensuite parvenir au destinataire le message et la clé, mais par des canaux différents pour plus de sécurité, afin que le destinataire, et seulement lui, puisse décoder le message. Ce chiffrement symétrique imposait donc d'avoir un canal sécurisé pour l'échange de la clé, ce qui dégrade sérieusement l'intérêt d'un tel système de chiffrement[15].

La cryptographie à clé publique (PKC : Public Key Cryptography) utilise deux clés ; une première, privée, l'autre publique. Ce système ne nécessite pas que les deux parties aient procédé à un échange préalable de la clé secrète pour communiquer. C'est donc beaucoup plus rapide. La publication de cette découverte par Deffie et Hellman, en 1976, a inspiré Rivest, Shamir et Adleman (RSA), chercheurs du MIT, qui y ont ajouté la signature numérique et qui ont publié leurs résultats, en 1977, dans la revue « Scientific American ». Ils offraient à toute personne intéressée d'envoyer par courriel le rapport complet de la méthode de chiffrement… d'où une sévère lutte de plusieurs années avec l'Agence de sécurité nationale des États-Unis qui voulait interdire cette diffusion intempestive à tout prix. Cet algorithme (RSA) servait encore en 2002 à protéger les codes nucléaires des armées américaine et russe[16].

Il y a plusieurs systèmes de chiffrement mais deux sont considérés comme des standards sur le marché : PGP (Pretty Good Privacy), fait par Philip Zimmermann qui a travaillé de 1984 à 1991 sur un programme permettant de faire fonctionner RSA sur des ordinateurs personnels[17] et S/MIME (construit à partir de la norme X509).



Lorsque l'on fait appel à un tel programme, c'est d'abord parce qu'on veut se prémunir contre la vulnérabilité de l'Internet où n'importe quel message peut être intercepté, lu, ou changé, sans que ni le destinataire, ni l'expéditeur n'aient nécessairement conscience du fait. Ce programme génère donc deux clés (ou fichiers d'ordinateur) en même temps pour les besoins de l'utilisateur. Une clé secrète que la personne gardera pour elle seulement sur une mémoire bien cachée, et une clé publique qu'elle pourra distribuer largement. Dans certaines organisations on utilise un serveur pour conserver les clés publiques de façon à ce que tout le personnel puisse consulter ce « bottin » et avoir accès aux clés. Ainsi, quand un individu veut envoyer un message confidentiel à une personne, il doit chiffrer le message à expédier à l'aide de la clé publique du *destinataire*, et ce dernier « *seulement* » peut ensuite utiliser sa clé privée et le déchiffrer. C'est donc totalement sécurisé car lui seul possède cette clé et même si ce fichier lui était volé, il y a toujours le long mot de passe (passphrase) qui, s'il est bien composé, est pratiquement impossible à décoder.

Valeur de preuve

Voilà pour la confidentialité, maintenant qu'en est-il de l'intégrité et de l'authenticité du document, conditions essentielles à sa valeur de preuve ?

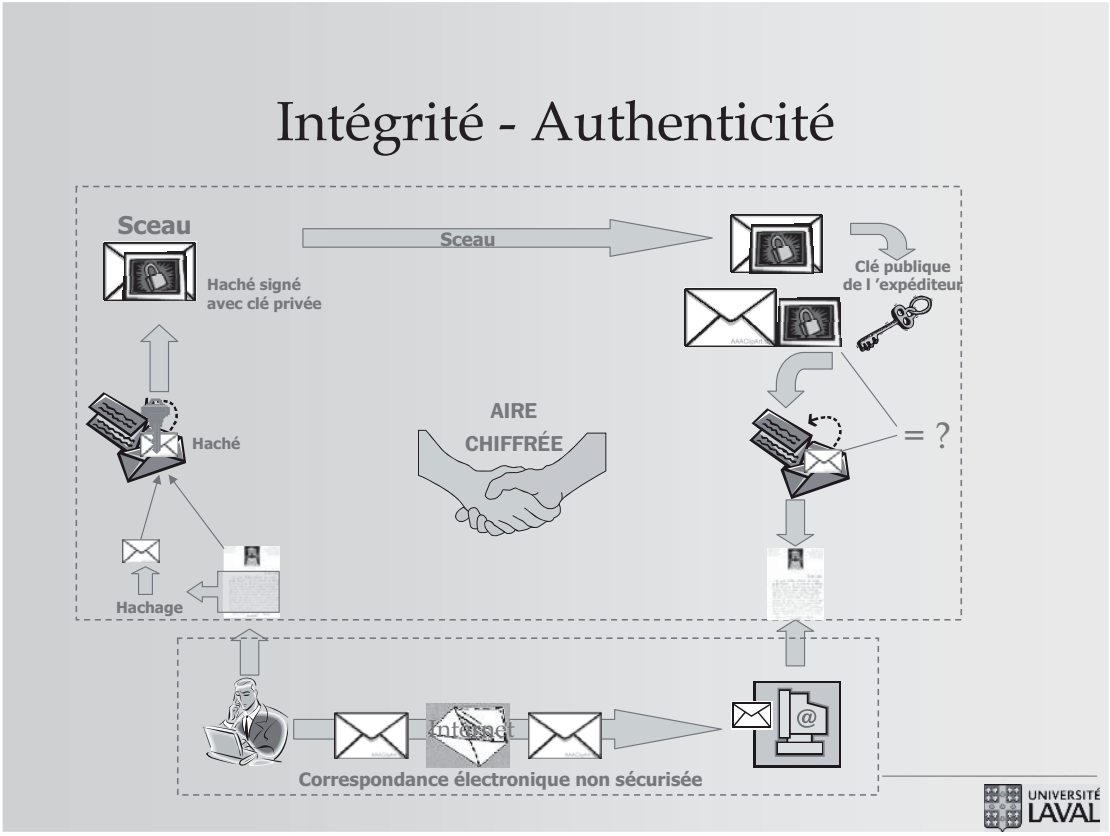
L'*intégrité* des données transmises par courriel consiste à déterminer si elles n'ont pas été altérées durant la transmission, soit de manière accidentelle, par un virus, ou de manière intentionnelle. Vérifier cette intégrité se fait en appliquant un algorithme ou fonction mathématique de cryptage et de compression communément nommée « hachage » (digest en anglais) qui nous permet d'obtenir le condensé d'un texte, c'est-à-dire une suite de caractères assez courte mais qui représente le texte en entier. Le résultat issu de cette opération est l'empreinte digitale ou numérique du fichier traité (ou haché). La fonction de hachage est telle qu'elle associe un et un seul haché à un texte en clair (cela signifie que la moindre modification du document entraîne la modification de son haché). Il s'agit d'une fonction à sens unique donc irréversible afin qu'il soit impossible de retrouver le message original à partir du haché.

Parmi les algorithmes de hachage les plus utilisés on retrouve le MD5 qui crée une empreinte de 128 bits et le SHA (pour Secure Hash Algorithm) qui crée des empreintes d'une longueur de 160 bits.

Il est important de comprendre que le hachage d'un document est toujours différent d'un document à un autre ; en effet, une clé ne voit dans un texte qu'une succession de 0 et de 1. Elle applique donc son algorithme et effectue l'échantillonnage complexe des 0 et des 1. Un texte très long peut ainsi prendre plus de vingt minutes à être « haché ». Après cette opération, la clé va couper le condensé au nombre de bits déterminé. Il s'agit de changer une virgule par un point virgule dans le texte original pour être assuré de la non conformité du hachage car la série de 0 et de 1 ayant été changée, l'algorithme en sera automatiquement altéré. Quand on associe cette empreinte numérique à un courriel, il suffit de calculer le haché du message reçu et de le comparer avec le haché accompagnant le document. Si le message (ou le haché) a été falsifié durant la communication, les deux empreintes ne correspondront plus. C'est ce qui va permettre de valider ou non l'*intégrité* du document.

Cette utilisation d'une fonction de hachage permet donc de vérifier que l'empreinte correspond bien au message reçu, mais ne prouve en rien que le message a bien été envoyé par celui que l'on croit être l'expéditeur. En effet, vérifier l'*authenticité* consiste à assurer, sans équivoque, l'identité de l'auteur d'un courriel, c'est-à-dire à garantir à chaque destinataire du message que l'expéditeur est bien celui qu'il croit être. C'est par la signature électronique que cette opération se réalise. Cette signature assure également une fonction de non-répudiation, c'est-à-dire qu'elle empêche l'expéditeur de nier avoir expédié le message.

Ainsi, si on reprend l'exemple précédent, l'expéditeur devra *signer* le haché à l'aide de sa clé *privée ce qui crée une véritable signature et qui est alors appelé un sceau* et va envoyer ce sceau au destinataire. À la réception du message, le destinataire déchiffrera le sceau avec la clé publique de l'expéditeur, puis le programme comparera le haché obtenu avec la fonction de hachage au texte reçu et déclarera cette comparaison correcte ou altérée.



Bien que cela semble affreusement complexe, et l'est effectivement, il faut se rappeler que les systèmes les plus efficaces traitent ces processus de façon transparente pour l'usager, le seul irritant étant le long mot de passe (passphrase) demandé à chaque fois que l'on veut envoyer une messsage signé. Une infrastructure à clé publique est déjà bien connue et développée. Il s'agit de celle du gouvernement du Canada qui repose sur les technologies Entrust.

Gestion et contrôle des documents produits ou transmis par courriel

Ayant pris connaissance des courriels reçus, ayant appliqué les actions nécessaires en toute validité, déchiffré les renseignements confidentiels ou nominatifs, et signé les réponses, etc., que reste-t-il à faire pour gérer adéquatement ces documents ?

- D'aucuns pourraient imprimer les courriels et leurs documents attachés, les relier et les classer dans le dossier sujet du poste de classement. Bien que cette stratégie soit encore utilisée, elle perd de plus en plus de popularité dans les habitudes de gestion et ne constitue plus une solution viable à long terme.
- D'autres personnes sont tentées de conserver les messages reçus ou envoyés dans l'application courriel afin de préserver les valeurs de preuve qui y sont maintenues. Pour s'y retrouver elles génèrent des boîtes thématiques basées sur leurs responsabilités ou activités propres. Il s'agit ici d'une solution intéressante mais qui très rapidement peut conduire à des difficultées de repérage dues au nombre de boîtes et de messages conservés.
- Enfin d'autres individus enregistrent leurs messages dans les espaces créés sur les disques selon le plan de classification de leur organisation et qui permettent de repérer l'ensemble des documents électroniques produits ou reçus par l'organisation. Il s'agit encore là d'une bonne pratique, car tous les documents électroniques sont colligés ensemble (notion la plus près possible de dossier complet) mais les messages ont perdu toute valeur de preuve car étant sauvegardés en format texte, il est donc possible de les éditer et d'y altérer les caractères autant dans le corps du message que dans l'en-tête ou toute autre partie.

Selon le Gartner Group, cité plus haut, 60 % des données essentielles ou critiques aux organisations transitent maintenant par le courriel et sont maintenues et conservées dans ces systèmes malgré le fait que ceux-ci n'ont pas été conçus pour remplir de telles fonctionnalités de gestion (Mayer 2003). Par ailleurs, Creative Networks Inc. de Palo Alta, Californie, affirme que seulement 29 % des organisations sont capables de retrouver un courriel de plus de 6 mois (Mayer 2003).

L'information institutionnelle est ainsi dispersée, partout dans l'organisation, dans les espaces personnels des utilisateurs (POP3), ce qui amène des coûts de recherche quelquefois exagérés. Plusieurs organisations « archivent » (comme leurs informaticiens le prétendent) sur des systèmes de « backups » sans pointeurs. Les « backups » peuvent « domper » tout un réseau sur quelques rubans. Le pire exemple de coût d'un document perdu a été raconté par John Montana de l'ARMA[18]. Il y racontait le cas d'une entreprise où les copies de sauvegarde sont régulièrement faites à partir de 3,000 terminaux. La compagnie a ainsi accumulé plus de 5,000 rubans de « backups ». Lorsqu'une poursuite de 22 millions de dollars s'est annoncée, ils ont dû « passer à travers » ces rubans pour retrouver le document qui leur manquait : ce qui leur a pris presque trois ans. Nous pouvons imaginer les coûts d'une telle opération !

Il n'est pas rare non plus de constater que bon nombre d'utilisateurs de micro-ordinateurs n'effectuent aucune copie de sécurité des documents ou fichiers qu'ils créent ou reçoivent par courrier électronique ou qu'ils disséminent très largement.

Plus les organisations sont imposantes, plus l'utilisateur est susceptible d'ignorer où sont véritablement ses fichiers de courriels et pire, les fichiers qui y sont attachés. Nous sommes donc confrontés au fait que ces documents sortent de la portée de la gestion de l'information, jadis bien contrôlée à l'intérieur des programmes de gestion de documents administratifs.

L'outil interroge donc fortement nos façons traditionnelles de traiter la correspondance. Mais pourquoi ne pas s'y référer, justement, à ces méthodes traditionnelles ?

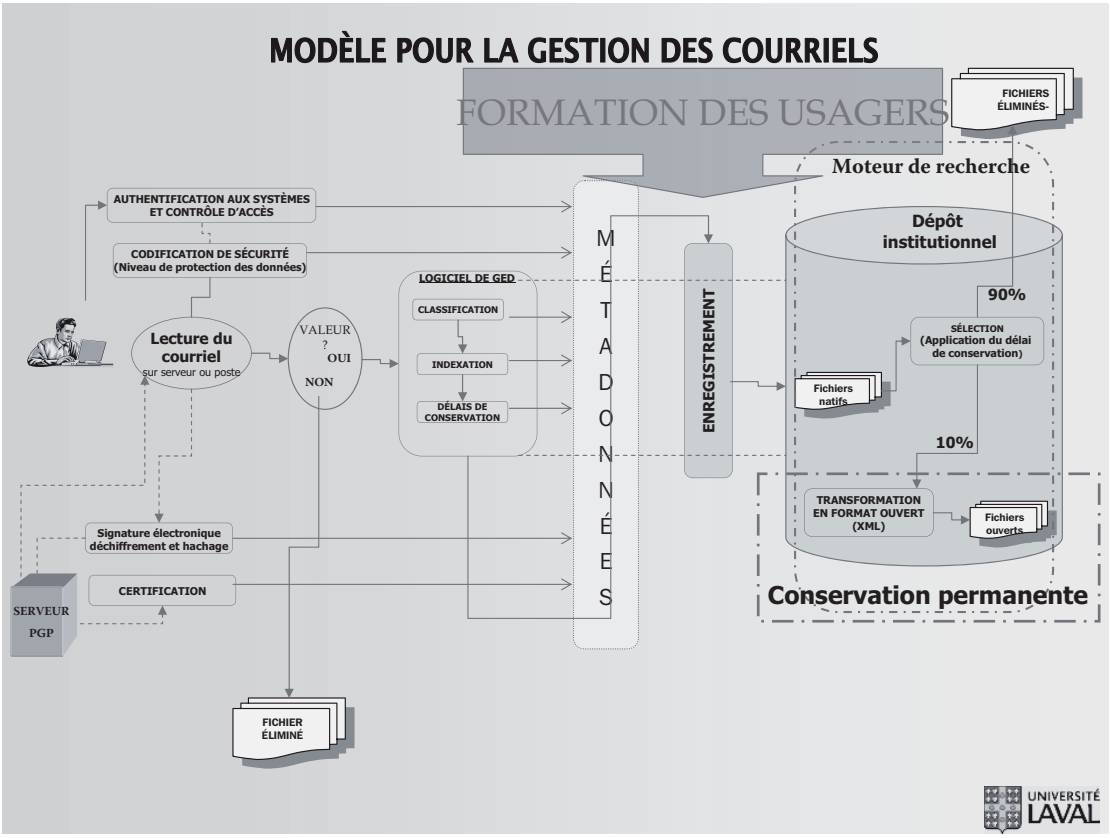
La gestion de la correspondance, quand elle était faite manuellement, consistait en un registre dans lequel on identifiait toute lettre reçue par l'officier en exercice (numéro unique), la date de sa réception, si la correspondance demandait une réponse, si oui à qui la lettre était transférée pour préparer la réponse, la date du transfert, la date où la réponse était attendue, la date effective de la réception de la réponse (tout le suivi) le nom de celui qui devait signer la réponse (pouvoirs de signer et délégation de pouvoirs) et enfin la date d'envoi de la réponse. De plus, la lettre était cotée afin de retracer les dossiers par sujets. Ces fameux registres chronologiques étaient ainsi créés et la lettre était classée au sujet.

Transposons donc le tout en électronique et tentons d'identifier les principes qui sous-tendent la notion d'enregistrement institutionnel des courriels, notion qui peut s'appliquer de fait à tous les documents administratifs numériques de l'organisation.

Il est important de noter d'abord que les registres de correspondance qui étaient tenus la plupart du temps par des secrétaires de direction, s'adressaient cependant aux gestionnaires ou officiers du bureau. Il s'agit donc ici d'envisager dès à présent que l'enregistrement institutionnel ne peut se concevoir sur des postes autonomes et disques locaux (des C) ; ils doivent être enregistrés sur des serveurs. En effet, l'enregistrement devient le processus par lequel une information consignée sur un support et reçue par une personne se transforme en un document institutionnel. Il s'agit donc du transfert d'une responsabilité individuelle à celle de l'organisation (en anglais, ce serait la différence entre document et Record).

L'enregistrement institutionnel, lorsqu'il est appliqué à la grandeur d'une organisation, permet de tenir un inventaire à jour des documents, diminue les risques de pertes des informations, permet la réutilisation des informations corporatives, leur mise en valeur et donc une saine gestion des connaissances dans l'organisation. Autres avantages, il favorise une normalisation des pratiques et assure un meilleur repérage des documents et dossiers. Bien entendu, pour implanter un tel système il faut une volonté claire de la direction à l'effet d'inscrire ce processus dans les priorités institutionnelles. Par ce geste, la direction d'une organisation démontrera clairement son appui à l'importance des objectifs visés, prémisse d'une plus grande réussite.

Cette réflexion sur la gestion des courriels, couplée à celle menée sur la gestion des documents numériques à l'intérieur des travaux de la Crepuq[19], m'a amenée à élaborer le modèle qui suit, résultant de l'analyse non pas d'un système précis, mais d'un système théorique ou conceptuel qui permet de mieux nous faire voir les capacités et possibilités reliées à l'enregistrement institutionnel.



Ce modèle tente d'illustrer le processus suivant : dès l'ouverture de l'ordinateur, un usager qui s'inscrit grâce à son nom et son mot de passe collige certaines informations permettant de l'identifier et d'assurer son environnement et sa sécurité. Ce simple geste fait en sorte de capter certaines métadonnées qui seront emmagasinées pour servir ultérieurement. Sans vouloir entrer dans les détails concernant les métadonnées – ceci n'étant pas notre propos – notons tout de même qu'elles sont là pour documenter tous les aspects du contenu, du contexte et de la structure des fichiers créés. Notons également qu'il est important que ces métadonnées soient autant que possible captées durant les processus, par la machine elle-même, de façon à ce que ces opérations demeurent transparentes pour les usagers, ce qui en fait un gage de plus de succès dans l'implantation du processus d'enregistrement institutionnel.

Il est possible d'ajouter, pour un poste ou un mandat particulier donné, une codification supérieure de sécurité qui ferait en sorte de chiffrer le poste ou de signer l'ensemble des courriels envoyés à partir de ce poste (par exemple le poste de secrétariat d'un rectorat ou de la présidence d'une compagnie). Voilà encore des métadonnées à colliger. Lorsqu'un courriel a besoin d'être chiffré ou déchiffré, certaines organisations peuvent bénéficier d'un « agent de certification interne » qui garantit l'identité des clés de chiffrement et des personnes. Si ce n'est pas le cas, elles peuvent utiliser les ressources d'un fournisseur externe.

Le processus doit ensuite permettre d'établir un contact avec la personne qui procède à la disposition ou à la fermeture du fichier électronique. Celle-ci devra s'interroger sur la valeur du fichier, valeur qu'elle devra interpréter à la lueur de son expérience, du contexte de création ou de réception, du cadre législatif ou réglementaire

ou de tout autre élément porté à sa connaissance. Si la réponse à ces questionnements se révèle être positive (valeur = oui), la personne procédera au classement du message grâce à un logiciel de gestion électronique des documents (GED) qui ajoutera automatiquement les métadonnées de classification, d'indexation et de délai de conservation.

Toutes ces métadonnées et le fichier seront alors intégrés dans le processus d'enregistrement au dépôt institutionnel, où les droits d'accès, la protection des données et le chiffrement, au besoin, seront maintenus, tant et aussi longtemps que les fichiers seront conservés en l'état de « semi-activité ». Dépendant de la disponibilité des ressources financières ou humaines de l'organisation, ils pourront demeurer en format natif – car moins coûteux – pendant les années de semi-activité ; en effet, ces périodes étant relativement courtes, les logiciels ne seront pas devenus obsolètes. Puis, la sélection sera faite grâce au calendrier de conservation pour en arriver à un total approximatif de 10 % seulement de fichiers ayant une valeur de conservation permanente. Ces fichiers seront alors convertis en un format plus adéquat pour la préservation à long terme (voir le point *Dernier défi : la préservation*).

Dès l'enregistrement institutionnel, un moteur de recherche puissant permettra le repérage des fichiers, selon le plus grand nombre possible de métadonnées. Voilà ce que ce modèle devrait dicter aux organisations qui veulent gérer adéquatement les documents numériques.

Implanter ces processus de gestion des documents

Les organisations, dans ce processus de rationalisation des pratiques documentaires électroniques, ne sont pas seules et peuvent bénéficier de guides. Ainsi la norme ISO 15489, développée à partir du standard australien (AS 4390) définit les exigences, les prérequis et les principes généraux d'un programme de gestion des documents numériques[20]. La norme détaille, entre autres, les étapes de l'évaluation, de la sélection des documents, de leur durée de conservation, de leur enregistrement, classement, stockage, accès et disposition. En faisant cela, elle met l'emphase sur le rôle des métadonnées dans ces processus. La norme recommande enfin le développement de mécanismes de suivi et d'audit du système et la formation des usagers.

La méthodologie esquissée par la norme ISO trouve également un complément dans le manuel DIRKS (Designing and Implementing Record Keeping System) qui, a été réalisé en support à la norme australienne, dès 1996, et qui lorsque cette dernière est devenue norme internationale, a été revu en incorporant les leçons de l'expérience australienne[21].

Comme la plupart des méthodologies, elle s'appuie, pour préserver les traces des activités de l'organisation, sur l'analyse de la fonction, de l'activité ou de la transaction qui génère le document et non sur ce document lui-même. C'est la préservation du contexte qui devient donc le point de départ de l'analyse, ce qui garantit la valeur des documents issus de l'activité. Cette première analyse est suivie de près par l'analyse des systèmes technologiques et des processus d'affaires.

Plus près de nous, le projet du gouvernement de l'Alberta, qui s'est appuyé sur les deux outils (ISO et DIRKS) se voulait d'abord et avant tout, comme DIRKS le recommande, une étude de cas (Alberta Government Services 2003). Leur publication « A Corporate Approach to Electronic Information Management » met en évidence les

besoins d'une gestion documentaire intégrant les courriels et note les avantages et désavantages de l'option d'impression des courriels et celle de gérer les courriels de manière électronique.

Le gouvernement du Québec également, dans la suite du Chantier en ingénierie documentaire, a développé une méthodologie et une stratégie de mise en place de la gestion des documents électroniques bien documentée dans son Cadre de référence gouvernemental en gestion intégrée des documents (GRDS 2004).

Enfin la CREPUQ, en février 2004, a concentré des efforts en ce qui a trait à la gestion des documents numériques, en publiant une étude réalisée pour les établissements universitaires (CREPUQ 2004) où elle développe un modèle de gestion et un plan d'action en sept étapes.

Dernier défi : La préservation

La notion de préservation à long terme ou d'archivage des fichiers numériques est pratiquement absente de la culture organisationnelle des institutions. Sauf dans de rares endroits, on ne se pose jamais la question de la pertinence de conserver ou d'archiver certains fichiers ou courriels ; encore moins celle de la durée de conservation requise en regard de la loi (calendrier de conservation des documents). Dans cette perspective, la gestion des courriels devient une question préoccupante, surtout depuis qu'à la décentralisation administrative s'est ajoutée une délégation de pouvoir et que les ordinateurs personnels possèdent des méga et même des giga-octets de mémoire leur permettant de stocker, sans outil spécifique de repérage, des milliers de documents.

Je n'aborderai pas en détail ce sujet qui pourrait faire l'objet d'un autre article tant il est important et complexe. Qu'il me soit seulement permis de souligner qu'une étude, menée en octobre 2002 par Maureen Potter dans le cadre d'un séminaire de formation de l'Erpanet, groupe européen mettant en commun les connaissances dans le domaine de l'archivage numérique, et qui s'intéresse au transfert de l'expertise entre les personnes et les institutions, porte particulièrement sur le XML et les options d'implantation pour les courriels (Potter 2002).

La communication de Potter examine également les approches de la migration de l'information et celles de l'émulation. Elle souligne la souplesse du XML et les avantages nombreux que ce format comporte en termes de description du contenu et du contexte, alors que la structure des fichiers peut également être préservée grâce à l'élaboration de balises bien structurées et d'une DTD (Document Type Définition). XML, allié à une feuille de style ou un formulaire de mémo, assure une recomposition de l'apparence du texte dans son format original[22]. Pour les courriels, étant donné leur format déjà normé, comme nous avons pu le constater avec les protocoles, c'est encore plus facile et les conversions s'effectuent rapidement et sûrement.

En conclusion, madame Potter énonce, en 2002 et cela ne s'est pas encore démenti, que le XML est sûrement une manière d'assurer une conservation à long terme des documents institutionnels. Elle appuie également sur le fait qu'une organisation qui entreposerait ses fichiers électroniques dans une voûte centrale en ce format serait en meilleure position pour reprendre le contrôle sur ses documents institutionnels et s'assurerait ainsi d'être en mesure de les repérer, les relire, les présenter pour preuve, de les utiliser quoi ! Au mieux et au bénéfice de sa mission et son mandat.

CONCLUSION

En terme de gestion des courriels et autres documents électroniques, les organisations font maintenant face à une situation paradoxale : plus ils bénéficient de systèmes technologiques performants, plus ils génèrent ou emmagasinent des documents, moins il sont capables de retrouver l'information pertinente et critique et plus le stress de leurs employés augmente. Le besoin de partage de l'information fait également en sorte que de multiples copies des documents sont faites sur une base régulière et distribuées par courriel, ce qui contribue à exacerber le problème de repérage, d'accès et de gestion des versions.

En 1997, une étude réalisée pour Pitney Bowes par l'Institute For The Future et Gallup démontrait que malgré le fait que les gestionnaires de compagnies recensées par Fortune 1000 recevaient et envoyaient plus de 178 documents par jour par toutes sortes de médias, aucune politique de communication ou guide n'existait en support pour aider ces employés dans le choix des outils de communication[23]. Pitney Bowes a poursuivi son sondage chaque année. Celui de 2000 confirmait la tendance avec encore plus de messages par jour et contribuait ainsi à une source de stress importante que sont les interruptions continuelles du travail au bureau. L'enquête révélait que sur une échelle de dix-huit sources de stress au bureau « comment se retrouver dans le courriel » arrivait en dixième position.

Bien sûr, il y a des problèmes d'utilisation du courriel et plusieurs sont causés par les usagers eux-mêmes[24]. En effet, certains n'utilisent pas de façon responsable cet outil de communication en ce sens que beaucoup trop de messages sont copiés pour information seulement et diffusés grâce à des listes de distribution importantes en nombre de correspondants. De plus, le changement de mentalités dans les entreprises de toutes natures fait que celles-ci tendent vers la prestation de services en ligne[25] ce qui contribue à augmenter le flux d'entrée des documents de cette nature. Il y a une grande différence, en termes de stress, entre pousser l'information sur l'écran de tous, et la rendre disponible à tous, soit dans un site ou dans l'intranet.

La plupart des grandes organisations en sont maintenant à examiner la possibilité de mettre en place des dépôts plus ou moins complexes de documents numériques incorporant toutes les fonctionnalités de la gestion des documents. Il n'en demeure pas moins qu'en ce qui concerne la gestion du courriel, une fois les courriels non sollicités ou inutiles éliminés, le plus grand défi reste la formation des personnes qui sont confrontées à ces courriels. Comme Mark Myers, spécialiste de la gestion des documents électroniques au Kentucky[26], le disait dans un courriel glané dans une liste de discussion au mois de février 2004 [je traduis] : « Il y a encore beaucoup de personnes qui gèrent leur courriel en l'imprimant sur papier. D'après nos expériences vécues depuis deux ans, le véritable défi est l'éducation, pas la technologie. Nous sommes effectivement en mesure de gérer adéquatement les documents électroniques, faire en sorte que les personnes nous les transmettent est le véritable problème ».

Carole Saulnier Directrice adjointe. Division des archives. Université Laval.

NOTES

1. Sur le site de la Wikipédia, l'encyclopédie vivante sur Internet, on situe plutôt cette date au 21 novembre 1969. Voir http://en.wikipedia.org/wiki/ARPANET
2. On raconte que ce fut par téléphone que les scientifiques devaient se confirmer le « login » d'une machine à l'autre et qu'à la première tentative, après l'envoi des trois premières lettres (L O G) les machines ont gelé !
3. Voir le site de Tomlinson à l'adresse : http://openmap.bbn.com/%7Etomlinso/ray/home.html
4. E-Mail and Groupware Servers *PC Magazine*, vol 23, Issue 3, 17 février 2004.
5. Pour des exemples de politique de courriel, on pourra consulter les URL suivants :

   Au Québec
   Chantier en réingénierie : http://www.tresor.gouv.qc.ca/doc/acrobat/ingenierie8.pdf
   Commission d'accès : http://www.cai.gouv.qc.ca/06_documentation/01_pdf/courrier.pdf

   Au Canada
   Administration fédérale : http://www.collectionscanada.ca/06/060404_f.html
   Alberta : http://www.im.gov.ab.ca/public/ManagingE-mailguide.pdf
   Colombie-Britannique : http://www.mser.gov.bc.ca/crmb/eimgmt/email.htm
   Terre-Neuve : http://www.gov.nl.ca/exec/treasury/itpolicy/email/default.htm
   Ressources naturelles Canada : http://www.nrcan.gc.ca/em-ce/emgd-f.htm
   Secrétariat du Trésor Canada – Sur l'utilisation du courriel dans les sites Web : http://www.cio-dpi.gc.ca/clf-nsi/inter/inter-04-tb_f.asp
   Pour plusieurs des politiques des états américains et autres gouvernements locaux consulter : http://www.coshrc.org/arc/states/res_emai.htm
6. METZ, Cade. 2004. Can e-mail survive? *PC Magazine* 23, 3 : 64-71.
7. Pour des statistiques sur le courriel, les virus et courriels non sollicités, voir le site http://www.postini.com/stats/
8. LAMMOTH, Friedhelm. 2005. L'avenir du marketing? Il sera multimédia, mobile, mesurable. *Magazine KMU*, n° 3.
9. La conséquence en est la chute annuelle de 5 milliards de lettres distribuées par la poste et la perte d'emploi très forte dans ce secteur. (Mayer 2003, 4).
10. Le Soleil, 29 avril 2004, p. A7.
11. Certains ont pensé imposer des tarifs à l'envoi de courriels de un dixième de cent (0.01¢) par courriel ou moins ce qui n'empêcherait aucune organisation d'envoyer tous les courriels requis dans l'exercice de ses fonctions ou de son mandat mais qui, pour une compagnie spécialisée dans l'envoi de millions des « spams » par jour, ferait en sorte d'éliminer naturellement plusieurs « compétiteurs du marché ».
12. *PC Magazine*, 23,3, 17 février 2004.
13. Cette problématique d'introduction aux défis liés à l'utilisation de documents électroniques est inspirée de nombreux écrits et réflexions qu'il m'a été donné de faire depuis 1996 dans l'exercice quotidien de mes fonctions tant à l'Université Laval qu'au sein de divers groupes de travail à la CREPUQ ou ailleurs. Parmi ces études notons *Le courrier électronique à l'Université Laval : Le présent et le futur*. Groupe de travail sur le courrier électronique, Université Laval, novembre 1996. 52p. ; Saulnier, Carole. *État de question sur la gestion des documents administratifs produits ou reçus par courrier électronique.* Université Laval, DAUL, juillet 1995. 7p. ; Saulnier, Carole. *Résumé de la position de la Division des archives en ce qui a trait à la gestion des documents numériques*. Université Laval, Groupe de travail sur la gestion et l'archivage des documents électroniques 1997. 8p. ; *Rapport du sous-comité sur l'intranet à l'Université Laval.* Université Laval, Sous-Comité sur l'intranet, Mars 2001. 58p. ; *Les portails informationnels à l'Université Laval. Rapport présenté au Comité de coordination des technologies de l'information (CCTI)*. Université Laval, Groupe de travail sur les portails informationnels. Mai 2002. 20p. ; ou encore CREPUQ. *La gestion des documents numériques des établissements universitaires du Québec : état de situation et planification stratégique*. Février 2004. 50 p.

14. L'histoire ne dit pas si cette société conservait le message original en scalpant ou coupant la tête du messager ! Pour de plus amples renseignements concernant l'histoire de la cryptographie, on pourra consulter Wikipédia, L'encyclopédie libre ou encore l'excellent ouvrage de Simon Singh (Singh 1999).

15. Un bon exemple de cette méthode est le fameux « Téléphone rouge » entre l'URSS et les États-Unis dont la clé passait par la valise diplomatique.

16. Pour une discussion concernant la sécurité relative au chiffrement par RSA on pourra consulter les sites suivants : http://library.thinkquest.org/27158/concept2_4.html et http://www.bibmath.net/crypto/moderne/indexmoderne.php3. Ce domaine évoluant très rapidement, on pourra consulter également le volume de Simon Singh, précédemment nommé, ou encore le site http://perso.wanadoo.fr/wakaziva/crypto/index.htm où l'avenir du chiffrement utilisant le protocole quantique et les photons (Quantum Key Distribution) est également expliqué.

17. Pour des renseignements sur Zimmerman ou le PGP, on pourra consulter le site personnel de Zimmerman à cette adresse : http://www.philzimmermann.com/EN/background/index.html

18. Le message était adressé par Montana de l'ARMA (Denver, Colorado) aux abonnés de la liste de discussion RECMGMT en octobre 1999. Le sujet en était « Costs of lost documents ».

19. Il s'agit du Groupe de travail sur les documents numériques (GGDN) du Sous-comité des archivistes de la CREPUQ. Les travaux du groupe ont contribué à la tenue d'une Journée d'étude ASGEU – CREPUQ, le 3 octobre 2003, à l'Université du Québec à Rimouski où les membres ont livré certaines pistes de solutions dans une conférence intitulée « Gestion des documents numériques : planification stratégique ». Le résultat des travaux a également donné lieu à la publication « La gestion des documents numériques des établissements universitaires du Québec : état de situation et planification stratégique », Sous-comité des archivistes, février 2004.

20. Voir le site http://www.naa.gov.au/recordkeeping/overview/summary.html

21. Le modèle méthodologique développé dans le manuel DIRKS illustre les étapes de la conception et de la mise en œuvre d'un système de gestion des documents. L'étape A permet d'avoir une vue d'ensemble de l'organisation et de positionner la gestion documentaire dans le contexte de cette organisation. Les étapes B et C permettent, en analysant les activités de l'organisme, d'identifier les processus d'affaires et les exigences et obligations de la tenue des dossiers dans l'organisation. Ce qui permet à l'étape D, l'évaluation des systèmes en place et l'identification des problèmes de la pratique courante. L'étape E identifie les stratégies à mettre en place pour répondre aux exigences documentaires. En F, la conception du système sera appuyée par l'analyse des prérequis et exigences documentaires et par les normes et politiques en vigueur. L'étape G, permet la mise en œuvre finale du système de gestion des documents qui devra être appuyée par une rétroaction avec les usagers. Enfin, l'étape H permet l'évaluation des capacités du système à remplir les attentes qui ont été définies lors de l'analyse des besoins et de la conception du système. La méthodologie enfin suggère plusieurs autres pistes et offre même un Guide pour le développement d'un projet pilote avec DIRKS et même un rapport coûts/bénéfices. Pour de plus amples renseignements concernant cette méthodologie, on consultera le site : http://www.naa.gov.au/recordkeeping/dirks/dirksman/contents.html

22. Pour lire un peu plus là-dessus, il est intéressant de consulter le projet des thèses électroniques mené à l'Université Laval et à l'Université de Montréal, en particulier le rapport sur le projet-pilote (Beaudry et Gauvin 2003).

23. *Managing Corporate Communications In The Information Age*, cité dans Gundry 2003.

24. On retrouve même, sur Internet, une campagne contre les « TUNA » (Totally Uninteresting News & Admin) où John Gundry, Directeur de Knowledge Ability Ltd en Grande-Bretagne (www.knowab.co.uk/ka), demande aux internautes de lui adresser les pires « TUNA » reçus. Il entend par cela les courriels inutiles envoyés par l'administration qui présentent par exemple la biographie d'un nouveau

directeur … à Tombouctou, des « Comment faire pour… réserver des salles de conférences » ou autres procédures semblables, des cours offerts contre le stress au bureau, et surtout les courriels du genre « Pour votre information » envoyés par des collègues qui font perdre du temps, qui noient les courriels importants sous l'avalanche et utilisent des ressources informatiques importantes de l'entreprise.

25. Par exemple, l'inscription des étudiants en ligne et leur confirmation d'admission, la soumission des rapports d'impôt, ou l'achat d'un produit et même sa réception, si le produit est virtuel.
26. Du Department for Libraries and Archives, Kentucky University.

BIBLIOGRAPHIE

ALBERTA GOVERNMENT SERVICES. 2003. Business case. A Corporate Approach to Electronic Information Management (EIM). In *Site du Gouvernement de l'Alberta,* [En ligne] http://www.im.gov.ab.ca/publications/pdf/BusCaseEIM.pdf (Page consultée en octobre 2005).

ARPANET. In *Wikipedia, The Free Encyclopedia* [En ligne]. http://en.wikipedia.org/wiki/ARPANET (Page consultée en octobre 2005).

BEAUDRY, Guylaine et Jean-François GAUVIN. 2003. *Rapport de la phase pilote du projet de publication et de diffusion électroniques des thèses de doctorat* [En ligne]. http://www.theses.umontreal.ca/theses/RapportThesesUdeM.pdf (Page consultée en octobre 2005).

COMMISSION DES COMMUNAUTÉS EUROPÉENNES. 2001. *Communications commerciales non-sollicitées et protection des données.* [En ligne]. http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/spamstudy_fr.pdf (Page consultée en octobre 2005).

CONFÉRENCE DES RECTEURS ET DES PRINCIPAUX DES UNIVERSITÉS DU QUÉBEC (CRÉPUQ). 2004. *La gestion des documents numériques des établissements universitaires du Québec : état de situation et planification stratégique.* [En ligne]. http://www.crepuq.qc.ca/documents/arch/Rapport-GGDN.pdf (Page consultée en octobre 2005).

CROCKER, Steve. 2000. Living Internet. History. In *The Living Internet.* [En ligne]. http://www.livinginternet.com/i/i.htm (Page consultée en octobre 2005).

CLYMAN, John. 2004. E-Mail Servers. *PC Magazine* 23, 3 : 85-95.

GROUPE DÉPARTEMENTAL DE RECHERCHE SUR LES DOCUMENTS STRUCTURÉS (GRDS). 2004. *Cadre de référence gouvernemental en gestion intégrée des documents.* [En ligne]. http://www.anq.gouv.qc.ca/conseil/crggid/crggid_accueil.htm (Page consultée en octobre 2005).

GUNDRY, John. 2002. Information (and E-mail) Overload. A Knowledge Ability White Paper. In *Knowledge Ability.* [En ligne]. http://www.knowab.co.uk/wbwload.pdf (Page consultée en octobre 2005).

HAUBEN, Michael. History of ARPANET. In *Site de l'Instituto Superior de Engenharia do Porto,* [En ligne]. http://www.dei.isep.ipp.pt/docs/arpa.html (Page consultée en octobre 2005).

Histoire de la cryptographie. In *Wikipédia, L'encyclopédie libre,* [En ligne]. http://fr.wikipedia.org/wiki/Histoire_de_la_cryptographie (Page consultée en octobre 2005).

History of the Internet. In *Wikipedia, The Free Encyclopedia,* [En ligne]. http://en.wikipedia.org/wiki/History_of_the_Internet (Page consultée en octobre 2005).

Introduction à la cryptographie. In *Comment ça marche.com.* [En ligne]. http://www.commentcamarche.net/crypto/crypto.php3 (Page consultée en octobre 2005).

MAYER, Paul. 2003. Email Storage & Management Best Pratices : A Regulatory & Business Requirement. Datalink. In *The Data Center Journal.* [En ligne]. http://www.datacenterjournal.com/Tools/WhitePapers/Email-White-Paper-new111.pdf (Page consultée en octobre 2005).

METZ, Cade. 2004. Can e-mail survive? *PC Magazine* 23, 3 : 64-71.

NATIONAL ARCHIVES OF AUSTRALIA et STATE RECORDS AUTHORITY OF NEW SOUTH WALES. 2000. Dirks Manual. In *Site des National Archives of Australia,* [En ligne]. http://www.naa.gov.au/recordkeeping/dirks/dirksman/contents.html (Page consultée en octobre 2005).

POSTINI INTEGRATED MESSAGE MANAGEMENT. *Postini Ressource Center – Message Threats.* [En ligne]. http://www.postini.com/stats/ (Page consultée en octobre 2005).

POTTER, Maureen. 2002. XML for Digital Preservation – XML Implementation Options for E-mails. In *Digitale Duurzaamheid.* [En ligne]. http://www.digitaleduurzaamheid.nl/index.cfm?paginakeuze=215&categorie=2 (Page consultée en octobre 2005).

SEGAL, Ben. 1995. A Short History of Internet Protocols at CERN. In *Site de l'International Federation of Library Association and Institutions,* [En ligne]. http://www.ifla.org/documents/internet/segb1.htm (Page consultée en octobre 2005).

SINGH, Simon. 1999. *Histoire des codes secrets : de l'Égypte des Pharaons à l'ordinateur quantique.* JC Lattès.

TOMLINSON, Ray. The First Network Email. In *Site de Ray Tomlinson,* [En ligne]. http://openmap.bbn.com/%7Etomlinso/ray/home.html (Page consultée en octobre 2005).