ÉTUDE

Les archives électroniques: la question de l'intégrité *

Taïk Bourhis

*P*lus que jamais, la question des archives électroniques préoccupe la communauté archivistique: l'abondante littérature sur le sujet en témoigne. Dans la plupart des organisations, une quantité toujours croissante d'informations est désormais créée et conservée uniquement sous forme d'enregistrements électroniques. Confrontés à cette nouvelle réalité, les archivistes s'efforcent de trouver des solutions aux problèmes particuliers que soulèvent les archives électroniques et doivent parfois revoir certaines de leurs méthodes et reconsidérer leur façon d'intervenir sur les documents. L'un des défis que doit relever la communauté archivistique est de se donner les moyens d'assurer la préservation à long terme de l'intégrité des données contenues dans les documents d'archives électroniques. Il est évidemment vital que celle-ci soit préservée pour que les archives électroniques, au même titre que les autres archives, puissent d'abord remplir leur fonction de preuve légale, administrative ou financière, et puissent ensuite être utilisées à des fins de témoignage ou encore d'information générale.

Dans le cas des archives sur support papier, divers systèmes et procédures ont été mis en place depuis fort longtemps afin de s'assurer que les documents demeurent fiables et authentiques. La signature (remplacée parfois par un symbole ou une croix), les sceaux et le recours aux services d'un officier public comme, par exemple, un notaire, constituent les principaux moyens reconnus et utilisés. Cependant, de telles méthodes ne sont évidemment pas applicables pour les archives électroniques et il est donc nécessaire de trouver d'autres alternatives.

L'objectif du présent article est précisément de déterminer quels sont les moyens possibles pour préserver l'intégrité des données contenues dans les documents d'archi-

* Cet article est une nouvelle version d'un travail réalisé à l'École de bibliothèconomie et des sciences de l'information, Université de Montréal, dans le cadre du cours BLT6621 *Recherche en archivistique* donné durant la session d'hiver 1999 par Jocelyne Martineau.

ves électroniques. Autrement dit, nous essaierons de voir comment il est possible de s'assurer que les données contenues dans les documents demeurent intactes et inchangées de façon à ce que leur fiabilité soit garantie. Nous ferons la synthèse des solutions proposées et des moyens concrets mis de l'avant dans la littérature afin de remédier à ce problème.

Pour commencer, nous définirons ce que sont les archives électroniques et mentionnerons leurs principales caractéristiques. Dans un deuxième temps, nous présenterons deux importants projets de recherche qui se sont intéressés à la question: il s'agit du projet de la *University of Pittsburgh* intitulé *Functional Requirements for Evidence in Electronic Record-keeping* et qui s'est déroulé de 1993 à 1996, et du projet de la *University of British Columbia* (UBC) intitulé *The Preservation of the Integrity of Electronic Records* et qui s'est déroulé d'avril 1994 à mars 1997. Nous ferons le bilan de ces deux projets en évaluant les solutions proposées et verrons que tous deux ont abordé différemment la question de l'intégrité. Nous présenterons également brièvement quelques projets d'implantation dont l'objectif était de vérifier les conclusions de l'un ou l'autre des deux projets. Dans un troisième temps, nous examinerons diverses solutions plus «techniques» empruntées à d'autres disciplines, en particulier à l'informatique, pour assurer l'intégrité des archives électroniques. Nous nous attarderons plus particulièrement aux possibilités qu'offrent la cryptographie, la signature électronique, le *digital time stamping* (sceaux électroniques) et le *hashing* à l'archivistique. Nous insisterons sur l'importance de travailler en collaboration avec d'autres disciplines pour mettre en place les meilleures solutions possibles.

La plupart des sources que nous avons consultées sont des articles de périodiques spécialisés en archivistique. Néanmoins, nous avons également utilisé quelques textes issus de revues du domaine de l'informatique. Les articles retenus sont très récents (ils ont tous été publiés dans les années 1990). Une telle sélection était nécessaire, puisque les changements dans le domaine de l'informatique sont extrêmement rapides et que les connaissances évoluent elles aussi rapidement. Comme la plupart des sources consultées sont en langue anglaise, il est nécessaire de s'attarder d'abord à quelques considérations terminologiques.

DÉFINITIONS ET CARACTÉRISTIQUES DES ARCHIVES ÉLECTRONIQUES

La terminologie employée dans le présent article nécessite quelques précisions. Pour commencer, nous avons choisi de traduire le terme anglais *electronic record(s)* par *document d'archives électroniques* et *archives électroniques*.

Nous considérons que le terme *archives* est celui dont le sens se rapproche le plus du terme *record(s)*. Comme le souligne Carol Couture dans son article intitulé «Le concept de document d'archives à l'aube du troisième millénaire[1]», le mot anglais *records*, pas plus que le mot anglais *archives*, n'est l'équivalent du terme français *archives*. Cependant, il n'existe pas de terme plus approprié et l'auteur souligne que le Conseil international des archives (CIA), notamment, a choisi de traduire *record(s)* par *document d'archives* et *archives*.

Par ailleurs, nous avons choisi d'utiliser exclusivement le terme *électronique* comme l'équivalent du terme *electronic*. En français, les auteurs utilisent souvent indifféremment les termes *archives électroniques* et *archives informatiques* pour exprimer plus ou moins la même réalité. Au Canada, l'expression *archives ordinolingues* est également employée, bien qu'on la rencontre moins fréquemment dans les textes plus récents. Nous avons choisi de ne pas utiliser le terme *archives informatiques*

puisqu'il peut revêtir pour certains un sens plus large que le terme *archives électroniques* et créer ainsi des ambiguïtés. En France, par exemple, les archives informatiques sont définies «comme étant l'ensemble des documents produits par l'informatique, quels que soient leur forme et leur support.[2]» Par conséquent, cette définition inclut notamment les documents d'archives sur support papier qui sont produits à l'aide de l'informatique, lesquels ne sont nullement considérés dans le cadre du présent article. De notre côté, nous avons choisi d'utiliser la définition d'archives électroniques proposée par l'Association française de normalisation (AFNOR) et dont le sens est plus restrictif: «Documents produits [ou reçus] par un organisme public ou privé dans l'exercice de ses activités et conservés sous forme d'enregistrements électroniques.[3]» Pour être plus complète, cette définition doit aussi s'appliquer aux personnes physiques (dans le cas des archives privées).

Les archives électroniques possèdent plusieurs caractéristiques particulières. Nous présenterons brièvement trois d'entre elles qui nous ont semblé avoir un impact direct sur la préservation de l'intégrité des documents: la dépendance vis-à-vis le système informatique et les diverses technologies, la facilité avec laquelle les données peuvent être effacées ou modifiées et la fragilité et la rapide désuétude des supports.

Pour Jacques Grimard, «la caractéristique principale des *archives électroniques* réside dans le fait qu'elles sont produites et accessibles seulement par le truchement d'instruments électroniques et qu'elles sont consignées sous forme de codes – numérique ou autres – sur des supports lisibles indirectement et exclusivement par le biais d'équipements de lecture appropriés.[4]» Un ordinateur est donc indispensable pour avoir accès à l'information. Le problème de la dépendance vis-à-vis les technologies se situe également à un autre niveau. Le domaine de l'informatique en général évolue à un rythme effarant: de nouveaux ordinateurs toujours plus performants sont sans cesse créés et de nouveaux logiciels (ainsi que des versions toujours plus récentes de ces logiciels) sont constamment mis sur le marché. Une partie importante du problème vient du fait que tout ce matériel et ces applications informatiques ne sont pas toujours compatibles entre eux. Il arrive également que certaines technologies soient vites dépassées et ne soient plus disponibles sur le marché de telle sorte que plusieurs documents d'archives électroniques ne peuvent pas être consultés si on ne dispose plus des technologies nécessaires.

Une autre des caractéristiques des archives électroniques qui nous intéresse particulièrement est le fait que l'information qu'elles contiennent est facilement manipulable. En effet, un document peut aisément être modifié, mis à jour, copié ou effacé sans que personne ne s'en rende compte, puisque aucune trace n'est laissée. Il est donc relativement difficile d'assurer l'intégrité et la sécurité de l'information. Pour l'instant, les organisations risquent de perdre des informations vitales pour leur bon fonctionnement si les données n'existent pas sur un autre support. Pour les mêmes raisons, il est également difficile d'assurer l'authenticité d'un document électronique. Actuellement, dans la plupart des pays, la question de la preuve légale des archives électroniques demeure toujours problématique et il est rare, même avec la signature électronique, qu'elles puissent servir de preuve probante.

Les supports pouvant contenir des archives électroniques sont très variés: cartes perforées (il s'agit de la première forme de support informatique et elles ne sont plus utilisées de nos jours) ; supports magnétiques (soit notamment les bandes, les rubans, les disquettes et les disques rigides) ; supports optiques (comme, par exemple, les *Compact Disc Read Only Memory*, plus communément appelés *Cd-Roms*). Tous ces supports sont généralement très fragiles et peuvent facilement se détériorer s'ils ne

sont pas conservés dans des conditions idéales. Comme les technologies évoluent rapidement, les supports deviennent également rapidement désuets et doivent être remplacés pour éviter de perdre des données importantes.

Ces différentes caractéristiques font des archives électroniques des documents difficiles à gérer. La communauté archivistique, de plus en plus sensibilisée au problème, a tenté d'apporter des solutions, notamment par la mise sur pied de deux importants projets de recherche.

PROJETS DE RECHERCHE SUR LES ARCHIVES ÉLECTRONIQUES

Sur le continent nord-américain, deux importants projets de recherche se sont intéressés spécifiquement à la question de l'intégrité des archives électroniques: celui de la *University of Pittsburgh* (*Functional Requirements for Evidence in Record-keeping*) et celui de la *University of British Columbia* (*The Preservation of the Integrity of Electronic Record*). L'objectif de cette section est de présenter brièvement ces deux projets et de faire le point sur les solutions proposées par chacun d'eux pour préserver l'intégrité des archives électroniques.

Le projet de la *University of Pittsburgh*: *Functional Requirements for Evidence in Electronic Record-keeping*

Le premier important projet de recherche sur les archives électroniques a vu le jour à la *School of Information Science* de la *University of Pittsburgh* en 1993. D'une durée de trois ans, ce projet a été financé par la *National Historical Publications and Records Commission* (NHPRC). Il a été dirigé par deux principaux chercheurs: Richard Cox et James Williams. Ceux-ci ont notamment été assistés par David Bearman, qui a agi à titre de consultant, ainsi que par des étudiants au doctorat, dont Wendy Duff et David Wallace.

Le principal objectif de ce projet était le suivant: «to explicitly define what requirements must be met by Record-keeping systems so that they [archivists] can intervene in organizational policy, systems design, and program implementation to ensure the creation of records, preserve their integrity and provide for access.[5]» Dans le cadre de ce projet, les archives électroniques étaient définies comme des «*evidence of transactions*». Cette définition tient compte du contenu du document, mais également de son contexte spécifique de création et de sa structure.

La première préoccupation a été de déterminer un ensemble de «conditions requises» ou «conditions fonctionnelles» (*functional requirements*) afin de s'assurer que les archives sous forme électronique puissent conserver leur fonction de témoignage. Pour y arriver, les participants au projet ont d'abord entrepris une vaste revue de la littérature. Ensuite, un groupe de travail chargé de réaliser une première ébauche de ces conditions requises a été mis sur pied. Les responsables du projet de la *University of Pittsburgh* ont choisi une méthode inductive. En effet, ils se sont basés sur des études de cas, des normes et des lois existantes et reconnues ainsi que sur des avis d'experts. Une première version des conditions requises a été distribuée au sein de la communauté archivistique et a été évaluée et commentée par elle. Finalement, les responsables du projet ont identifié une série de dix-neuf conditions requises. Elles ont été regroupées en trois catégories: 1) Celles reliées à l'organisation (*Conscientious Organisation*), 2) Celles reliées au système de gestion des documents d'archives (*Accountable Record-keeping Systems*), 3) Celles reliées aux documents d'archives eux-

mêmes (*Captured Records*, *Maintained Records* et *Usable Records*). La première catégorie est constituée d'une seule condition requise (*Compliant*) qui précise qu'une organisation doit connaître et respecter les lois, les règlements, les normes et les pratiques professionnelles reconnues qui la concernent directement. Les conditions requises de la deuxième catégorie (*Responsible*, *Implemented*, *Consistent*) visent à s'assurer que les archives électroniques soient gérées par un système de gestion des documents d'archives fiable. Finalement, la troisième catégorie comprend les caractéristiques que les archives électroniques doivent posséder de façon à ce que leur intégrité soit préservée: *Comprehensive*, *Identifiable*, *Complete (Accurate*, *Understandable*, *Meaningful)*, *Authorized*, *Preserved (Inviolate*, *Coherent*, *Auditable)*, *Removable*, *Exportable*, *Accessible (Available*, *Renderable*, *Evidential)*, *Redactable*. L'annexe 1, tirée de l'article de Wendy Duff intitulé «Ensuring the Preservation of Reliable Evidence: A Research Project Funded by the NHPRC», présente de façon schématique les *functional requirements*.

Selon l'équipe du projet de la *University of Pittsburgh*, un système de gestion des documents d'archives doit rencontrer ces diverses conditions pour que soit préservée l'intégrité des archives électroniques. Cependant, comme l'explique Margaret Hedstrom dans son article intitulé «Building Record-keeping Systems: Archivists Are Not Alone on the Wild Frontier», des études ultérieures ont démontré que ces conditions n'avaient pas toutes la même importance et que, dans le cas de certaines organisations, quelques-unes d'entre elles s'avéraient même inappropriées, inutiles ou encore trop dispendieuses.

Outre la liste des conditions requises, trois autres documents ont été produits dans le cadre de ce projet: le *literary warrant*, les *production rules* et les *metadata specifications*. Le *literary warrant* est constitué d'une série d'énoncés, lesquels viennent appuyer les conditions requises. Ces énoncés consistent en une compilation de lois, de normes, d'autres règles et de pratiques professionnelles de différentes disciplines. Ils spécifient notamment quels documents doivent obligatoirement être préservés pour leur fonction de témoignage et de preuve et combien de temps ils doivent être conservés.

Les règles de production (*production rules*), quant à elles, énoncent les conditions requises de façon à ce que les éléments qu'elles contiennent soient clairement identifiables et compris par le système informatique. Pour établir les règles de production, les responsables du projet ont utilisé une technique empruntée au domaine de l'intelligence artificielle: « the production rule knowledge representation ». Plus précisément, les règles de production consistent en un ensemble de *Horn clauses*. Une *Horn clause* est un énoncé qui s'exprime sous la forme « si … alors … ». Par exemple, A est considéré vrai seulement si B et C et D sont vrais (autrement dit, si B et C et D alors A). Cet énoncé est représenté de la façon suivante:

<A>: <B><C><D>

Ce langage particulier « … enables the researchers to state each specification in such a way that it is recognizable and when implemented will be observable and therefore testable within a system[6]». Afin d'illustrer concrètement en quoi consiste ces *production rules*, en voici un extrait:

<RECORDKEEPING_REQUIREMENTS Satisfied>:

<ORGANIZATION Compliant>

<SYSTEM Accountable>

<RECORDS Functional>

<ORGANIZATION Compliant> (1.0):

<EXTERNAL_REQUIREMENTS Known> (1.0a)

<Linked EXTERNAL_REQUIREMENTS INTERNAL_RULES> (1.0b)

<Updated EXTERNAL_REQUIREMENTS INTERNAL_RULES> (1.0c)

<EXTERNAL_REQUIREMENTS Known> (1.0a):

LAWS Identified>(1.0a1)

REGULATORY_ISSUANCES Identified> (1.0a2)

BEST_PRACTICES Identified> (1.0a3) ...[7]

Finalement, un modèle méta-informationnel (*metadata specifications*) découlant des conditions requises et des règles de production a été établi. Il s'agit d'un ensemble d'éléments d'information qui identifient chaque document d'archives et en décrivent le contenu, la structure, le contexte de création et l'utilisation future.

Le schéma de l'annexe 2 illustre la façon dont chacun des quatre documents produits dans le cadre de ce projet sont reliés entre eux et forment un tout. Les conditions requises sont bien évidemment au cœur de ce tout.

Le projet de la *University of British Columbia*: *The Preservation of the Integrity of Electronic Records*

Le second important projet de recherche sur les archives électroniques, celui de la *University of British Columbia*, a été réalisé dans le cadre du programme de maîtrise en archivistique offert à la *School of Library Archival and Information Studies* (SLAIS) de cette université. Il a été financé par le Conseil de recherche en sciences humaines du Canada (CRSH) et s'est déroulé d'avril 1994 à mars 1997. L'équipe de recherche était composée de Luciana Duranti (chercheure principale), Terry Eastwood (chercheur associé) et Heather MacNeil (assistante de recherche).

Le but premier du projet était le suivant: «to identify and define in a purely theorical way both the byproducts of electronic information systems and the methods for protecting the integrity [meaning the reliability and authenticity] for those wich constitute evidence of action[8]». De cet objectif principal découlaient six objectifs spécifiques, lesquels sont présentés à l'annexe 3 du présent article. Dans le cadre de ce projet, un document d'archives est défini comme «any document created by a physical or juridical person in the course of practical activity».

Pour parvenir à ses fins, l'équipe de recherche a utilisé une approche déductive. Elle est d'abord partie d'un ensemble de prémisses généraux concernant la nature des documents d'archives. Elle a ensuite cherché à déterminer si ceux-ci étaient toujours valides dans un environnement électronique. Les participants au projet ont basé leur étude sur les principes et les concepts de la diplomatique et de l'archivistique. Le *Dictionnaire des archives : de l'archivage aux systèmes d'information* de l'AFNOR définit la diplomatique comme la «science qui étudie les actes écrits en eux-mêmes (et par extension, tous les documents d'archives), d'après leur forme, leur genèse et leur tradition[9]». Comme le souligne Luciana Duranti, elle a été développée aux XVII^{e} et XVIII^{e} siècles dans le but de prouver la fiabilité et l'authenticité des documents[10]. Alors que la diplomatique étudie les documents d'archives comme entités individuelles, l'archivistique s'intéresse aux documents d'archives en tant qu'ensembles. En effet, l'archivistique se préoccupe davantage de déterminer la façon dont sont reliés entre

eux les documents d'archives et la manière dont ceux-ci peuvent être organisés et diffusés.

L'analyse conceptuelle a constitué une étape importante du projet. L'équipe de recherche s'est penchée plus particulièrement sur la définition de trois termes: document d'archives (*record*), fiabilité (*reliability*) et authenticité (*authenticity*). Luciana Duranti explique que «at the heart of diplomatics lies the idea that all records can be analyzed, understood, and evaluated in terms of a system of formal elements that are universal in their application and decontextualized in nature[11]». Les documents doivent par conséquent être définis par les éléments qui déterminent leur structure et non pas les éléments d'information qu'ils contiennent. Dans le cadre de ce projet, il a été démontré que les archives électroniques, tout comme les documents d'archives traditionnels, sont constitués de sept éléments formels: un médium (ou support d'information), une forme, des personnes impliquées, une action, un contexte, un *archival bond* (ce qui relie un document d'archives au précédent, au suivant et à tous les autres qui sont le produit de la même action ou activité) et un contenu. Luciana Duranti explique qu'à la différence des documents d'archives traditionnels, les différentes composantes des archives électroniques ne sont pas liées entre elles de façon inextricable et elles peuvent être traitées et gérées séparément.

Luciana Duranti a également consacré un article à la définition de deux concepts centraux du projet: la fiabilité et l'authenticité[12]. Pour elle, la fiabilité fait référence à l'autorité et à la fidélité d'un document d'archives. Celui-ci doit rendre compte d'un fait en lui-même. Par exemple, un certificat de citoyenneté fiable doit pouvoir prouver que la personne en question est citoyenne d'un pays. Pour s'assurer de la fiabilité d'un document, l'archiviste doit exercer un contrôle sur sa forme et son processus de création. L'authenticité, de son côté, garantit que le document n'a pas été manipulé, substitué ou falsifié après qu'il ait été complété par son créateur initial (ou ses créateurs initiaux) et qu'il est bien le document qu'il est censé être. L'authenticité repose donc sur la manière dont l'information a été transmise et préservée à travers le temps.

Partant de cette analyse conceptuelle, les chercheurs ont établi une série d'hypothèses, lesquelles déterminent les composantes nécessaires pour s'assurer que les archives électroniques demeurent complètes, fiables et authentiques. Ces hypothèses ont été formulées dans les réponses apportées à huit grandes questions (*templates*): 1. What is a record in the traditional environnement? 2. What is a complete record in the traditional environnement? 3. What is a reliable record in the traditional environnement? 4. What is an authentic record in the traditional environnement? 5. When is a record created in the electronic environnement? 6. When is a complete record created in the electronic environnement? 7. How is a record created reliable in the electronic environnement? 8. How is an electronic record guaranteed and / or proved authentic?[13]

Les conclusions du projet de la *University of British Columbia* peuvent être regroupées en deux principales catégories. Premièrement, des méthodes spécifiques et des conditions requises pour assurer la préservation de l'intégrité des archives électroniques ont été établies. En effet, il a été déterminé que la fiabilité et l'authenticité des archives électroniques étaient mieux assurées lorsque des règles et des procédures régissant l'ensemble du système de gestion des documents d'archives (quel que soit le support) étaient établies ; que la fiabilité et l'authenticité étaient mieux garanties lorsqu'on accordait une attention particulière au contexte documentaire des archives électroniques, c'est-à-dire aux relations qui existent entre les documents d'un même fonds (d'où l'importance de réaliser avec soin la classification, les enregistrements et

les descriptions) ; que la fiabilité et l'authenticité ne pouvaient être préservées que si les archives électroniques étaient traitées et gérées ensemble avec les autres archives du fonds auxquelles elles appartiennent.

Deuxièmement, des considérations générales concernant la maintenance et la préservation de documents d'archives fiables et authentiques ont été établies. Pour commencer, en ce qui concerne la préservation de l'intégrité des archives électroniques, le cycle de vie des archives peut être divisé en deux phases: une première phase durant laquelle on se préoccupe du contrôle de la création et de la maintenance de documents actifs et semi-actifs fiables et authentiques, et une seconde phase durant laquelle on se préoccupe de la préservation de documents inactifs authentiques. Ensuite, il a été déterminé que l'intégrité des archives électroniques était mieux préservée si l'on confiait au créateur la responsabilité d'assurer leur fiabilité et à la personne ou à l'organisation chargée de la préservation la responsabilité d'assurer leur authenticité.

Il est intéressant de noter que le *International Research on Permanent Authentic Recors in Electronic Systems Project* (*InterPARES Project*) qui est actuellement en cours est basé sur les concepts retenus et / ou élaborés dans le cadre du projet de la *University of British Columbia*. Comme l'a expliqué Luciana Duranti dans une conférence qu'elle a donnée en juin 2000 lors du 29e Congrès de l'Association des archivistes du Québec, l'objectif de ce projet est cependant différent puisqu'il « vise à formuler des critères pour développer des procédures, des stratégies et des standards internationaux, nationaux et institutionnels en vue de la conservation à long terme des documents électroniques authentiques[14] ».

Bilan des deux projets

Le projet de recherche de la *University of Pittsburgh* et celui de la *University of British Columbia* avaient en commun le même objectif général: celui de préserver l'intégrité des archives électroniques. Néanmoins, les perspectives adoptées par chacun d'eux sont fondamentalement différentes. Pour commencer, la façon dont sont définies les archives électroniques n'est pas du tout la même d'un projet à l'autre. Le projet de la *University of Pittsburgh*, rappelons-le, définit les archives électroniques comme des «evidence of transactions». Le projet de la *University of British Columbia*, de son côté, conçoit les documents d'archives dans des formes et des contextes plus divers. La définition proposée par le projet de la *University of Pittsburgh* est donc plus restrictive. Cette différence au niveau de la terminologie a évidemment eu des conséquences sur la façon d'aborder la problématique des archives électroniques et sur les conclusions des projets.

Nous avons vu que les méthodologies employées dans le cadre des deux projets étaient fort différentes. Les chercheurs ayant participé au *Functional Requirements for Evidence in Electronic Record-keeping Project* de la *University of Pittsburgh* ont choisi une approche déductive et ont ainsi basé les *functional requirements* sur un ensemble de normes et de pratiques qui ont vu le jour dans un contexte juridique particulier. Par conséquent, les méthodes proposées pour développer un système de gestion des archives permettant d'assurer l'intégrité des archives électroniques s'appliquent davantage à des milieux spécifiques. En effet, la *literary warrant*, sur laquelle repose les *functional requirements*, consiste en un ensemble de lois, de normes et autres règles particulières dont la majorité sont issues de l'expérience américaine. Au contraire, le projet de la *University of British Columbia* a opté pour une approche

déductive et, en se basant sur les théories et les méthodes de la diplomatique et de l'archivistique, en est arrivé à des conclusions qui sont davantage universelles. Le modèle qu'il propose est donc plus général et peut s'appliquer à des contextes plus divers.

Une autre différence fondamentale entre les deux projets réside dans la façon dont sont réparties les responsabilités de la gestion des archives électroniques tout au long du cycle de vie des archives. Dans le cas du projet de la *University of Pittsburgh*, qu'il s'agisse d'archives courantes, intermédiaires et définitives, les *functional requirements* s'appliquent de la même façon. De plus, le modèle présenté par les chercheurs implique une intégration complète des responsabilités relatives à la gestion des archives électroniques, y compris les responsabilités financières et juridiques. Le projet de la *University of British Columbia*, de son côté, différencie les besoins des archives courantes et intermédiaires de ceux des archives définitives et, nous l'avons vu, prévoit un partage des responsabilités quant à leur gestion.

Les quelques différences entre les deux projets que nous venons de présenter brièvement ne sont évidemment pas exhaustives, mais elles donnent une idée générale de l'orientation prise par chacun d'eux et permettent de mieux comprendre les solutions proposées pour préserver l'intégrité des archives électroniques.

Finalement, il importe de souligner que ces deux importants projets ont donné lieu à d'autres initiatives ayant pour objectif de trouver des solutions aux problèmes posés par les archives électroniques. En effet, divers projets ont été mis sur pied en vue de mettre en application certains éléments – en particulier les *functional requirements* – proposés par le projet de la *University of Pittsburgh* et celui de la *University of British Columbia*. Dans son article intitulé «Building Record-Keeping System: Archivists Are Not Alone on the Wild Frontier», Margaret Hedstrom présente brièvement quatre d'entre eux: le *Philadelphia's Electronic Records Project* (PERP), le *Indiana University Electronic Record Project*, le *Models for Action Project* (il s'agit d'un projet réalisé conjointement par le *New York State Center for Technology in Governement* et le *State Archives and Records Administration*) et le projet de la *DoD Records Management Task Force*. D'autres travaux ont également été entrepris en vue de tester et de s'assurer de la pertinence des *functional requirements*, dont le projet de la *World Bank* et le *Vermont State Archives Electronic Record Project*.

Chacun de ces projets pilotes et de ces études se sont intéressés à des aspects particuliers des deux grands projets. L'équipe du *Philadelphia Electronic Records Project*, par exemple, a notamment cherché à développer une méthode permettant d'utiliser des métadonnées pour gérer les archives électroniques lors des différentes transactions de l'organisation et ce, en se basant sur le modèle développé par la *University of Pittsburgh*. Le projet de la *World Bank*, de son côté, s'est basé sur la *literary warrant* pour évaluer des systèmes de gestion de documents. La *University of Indiana*, quant à elle, s'est notamment donné pour objectif d'évaluer les systèmes existants en fonction des *functional requirements* et de voir s'ils y répondaient.

Comme le souligne Margaret Hedstrom, il est difficile de tirer des conclusions générales au sujet de tous ces projets tant les organisations dans lesquelles des expériences ont été tentées étaient différentes, sans compter que la portée, les objectifs et les perspectives adoptés par chacun d'eux étaient très diversifiés. Un des points qu'elle soulève est le fait que pour chacun des projets, les organisations en cause avaient tendance à vouloir simplifier les modèles et à ne retenir que les *functional requirements* qui répondaient véritablement à leurs besoins. Il semble donc que les

modèles développés par la *University of Pittsburgh* et la *University of British Columbia* aient besoin d'être adaptés en fonction de l'organisation où ils sont implantés. Des études en cours et des projets futurs permettront certainement de les améliorer et de les rendre davantage efficaces dans les différents contextes. Pour le moment, les projets pilotes mentionnés ci-haut montrent que les modèles développés par les deux principaux projets (et parfois la combinaison de plusieurs de leurs éléments) contribuent à assurer l'intégrité des archives électroniques en imposant un certain nombre de conditions requises pour la création, la gestion et la conservation de ces archives.

Si des projets pilotes sont en train de démontrer la pertinence de tels modèles pour tenter de répondre à la question de l'intégrité des archives électroniques, les solutions proposées par d'autres disciplines sont parfois négligées par les archivistes. Ce sont quelques-uns de ces moyens plus «techniques» que nous nous proposons d'examiner dans la prochaine partie.

MOYENS «TECHNIQUES» POUR ASSURER L'INTÉGRITÉ DES ARCHIVES ÉLECTRONIQUES

Les différents projets de recherche sur les archives électroniques prouvent bien que les archivistes sont de plus en plus sensibilisés à la question de l'intégrité et qu'ils s'efforcent de trouver des solutions. Cependant, ils sont parfois peu familiers avec les moyens développés et mis en place par les autres disciplines qui sont confrontées à des problèmes semblables. Margaret Hedstrom souligne que cette tendance qu'ont certains archivistes à se replier sur eux-mêmes comportent quatre importantes implications: 1) Les archivistes peuvent ne pas prendre conscience du potentiel des différents systèmes, méthodes et techniques développés par les autres disciplines qui ont des préoccupations similaires en ce qui concerne l'authenticité, l'intégrité et la préservation des documents ; 2) Il peut arriver que soient développés des modèles conceptuels et des méthodes qui sont théoriquement très valables sur le plan archivistique, mais qui sont techniquement impossibles à mettre en application ou encore trop dispendieux ; 3) Comme le délai entre le moment où les recherches sont entreprises et le moment où les résultats sont disponibles est souvent long, les travaux qui reposent sur des hypothèses impliquant des moyens technologiques courants ou des politiques organisationnelles en vigueur peuvent être déjà dépassés quant vient le moment d'implanter les solutions trouvées ; 4) Les archivistes peuvent manquer une opportunité de participer à la réorganisation d'un système et d'exercer ainsi une influence sur les nouvelles orientations prises au sein d'une organisation[15].

Depuis un certain nombre d'années, différents outils et techniques ont été développés par d'autres disciplines, en particulier l'informatique, pour assurer la sécurité, la confidentialité, l'authenticité et l'intégrité de documents électroniques. Parmi ceux-ci, nous avons choisi de nous intéresser à la cryptographie, à la signature électronique, au *digital time-stamping* et au *hashing*.

La cryptographie

La cryptographie (ou chiffrement) constitue l'un des moyens que les archivistes peuvent prendre en considération pour assurer l'intégrité des archives électroniques. Le *Dictionnaire des archives : de l'archivage aux systèmes d'information* de l'AFNOR définit la cryptographie comme la «technique permettant de rendre par codage un texte inaccessible à ceux qui n'en sont pas les destinataires ou qui ne disposent

pas de la clé ou du chiffre[16]». Ainsi, le cryptage consiste à convertir un message original (*plaintext*) en un message codé (*ciphertext*). Par opposition, le décryptage est la conversion d'un message codé en un message original. Pour crypter un message (ou un document d'archives), un ou plusieurs algorithmes sont utilisés. Un algorithme se définit comme «l'ensemble des règles opératoires propres à un calcul ou à un traitement informatique[17]». Un algorithme est activé par une clé. Cette dernière joue un rôle central puisqu'elle seule donne accès au contenu du message.

Il existe différents types de cryptographie. Premièrement, la cryptographie classique (ou à clé secrète) se caractérise par le fait qu'elle utilise une seule et même clé pour le cryptage et le décryptage. Elle pose certains problèmes dans le cas d'envois de messages puisqu'elle implique que le destinataire possède préalablement la clé utilisée par l'expéditeur. En effet, il serait inutile d'envoyer d'abord un message crypté et ensuite la clé permettant de le décrypter par le même canal de communication: la sécurité, l'authenticité, la confidentialité et l'intégrité du message ne seraient plus garanties. Cependant, si l'expéditeur et le destinataire sont les seuls à connaître la clé, l'intégrité du message est assurée, puisque si le message est altéré après avoir été crypté, il devient indéchiffrable.

Élaborée en 1976 par W. Diffie et M. E. Hellman, la cryptographie à clé publique (ou asymétrique) résout les problèmes posés par la cryptographie à clé secrète. Elle fonctionne avec une combinaison de clés publiques et de clés secrètes complémentaires. Pour crypter le message, l'expéditeur utilise sa clé secrète. Pour décrypter le message, le destinataire utilise la clé publique (complémentaire) de l'expéditeur, laquelle est publiée et rendue accessible à tous. L'authenticité et l'intégrité sont assurées, puisque, s'il arrive à déchiffrer le message, le destinataire peut avoir la certitude de l'identité de l'expéditeur (qui est le seul à connaître la clé secrète) et du fait que le message n'a pas été altéré après avoir été crypté. S'il veut assurer la confidentialité d'un message, l'expéditeur peut également choisir d'utiliser la clé publique du destinataire. De cette façon, seule la personne qui détient la clé secrète complémentaire pourra y avoir accès. L'expéditeur peut ainsi avoir la certitude que seul le destinataire choisi sera en mesure de lire le message. L'annexe 4 illustre le fonctionnement de la cryptographie à clé publique.

Le cryptosystème le plus connu est le RSA. Il a été développé par Rivest, Shamir et Adelman en 1978. Il permet à chaque individu ou organisation qui publie sa clé publique par l'intermédiaire d'une autorité reconnue et fiable (*trusted authority*) d'avoir sa propre clé secrète, laquelle ne changera pas. Bruce Schneier fait remarquer que la cryptographie constitue un moyen relativement sécuritaire, puisqu'elle est aujourd'hui à ce point développée qu'il n'est pas possible de calculer une clé privée à partir de la clé publique correspondante (cela prendrait quelques milliers d'années)[18].

Comme l'explique Alan Poulter dans son article intitulé «Cryptography and records management», la cryptographie est un des moyens que l'archiviste peut envisager à la fois pour la conservation et la transmission de documents d'archives sous forme électronique. En effet, il est possible de conserver des fichiers électroniques cryptés selon les méthodes décrites ci-haut et d'en contrôler l'accès en veillant à la sécurité des clés qui permettent de les reconstituer. De cette façon, personne ne pourra porter atteinte à leur intégrité. Il existe d'ailleurs sur le marché des logiciels qui permettent de crypter automatiquement les fichiers qui sont sauvegardés sur un disque dur. L'intégrité du document repose donc en grande partie sur sa sécurité. L'archiviste qui a recours à une telle méthode doit, par conséquent, être prudent. La question de la gestion des clés constitue un des principaux problèmes auquel il sera confronté. Afin

d'éviter que les clés ne soient perdues, volées, mal utilisées ou oubliées, il est essentiel de développer des méthodes de vérification et d'assurer un contrôle sur la diffusion des clés.

La cryptographie peut également s'avérer fort utile pour assurer l'intégrité des documents lors de transmissions électroniques des données, que ce soit par courrier électronique ou par transfert de fichiers. L'une des solutions présentées par Alan Poulter est le PGP (*Pretty Good Privacy*). Il s'agit d'une application informatique gratuite qui permet de crypter des documents électroniques en utilisant notamment la signature électronique. Elle est utilisée en particulier pour le courrier électronique, mais s'applique également aux autres types de documents qui se présentent sous forme électronique. Pour préserver l'intégrité de ce type de documents électroniques, les archivistes peuvent notamment se baser sur les progrès faits du côté de l'EDI (*Electronic Data Interchange* ou Échange de données informatisées). L'EDI se caractérise notamment par le fait qu'il permet des échanges sécuritaires de données sous forme électronique, lesquels se font bien souvent sans intervention humaine. En effet, l'EDI assure la plupart, voire toutes les opérations d'une transaction, que ce soit, par exemple, la création, la transmission et l'interprétation des données. Par ailleurs, comme le souligne Serge Parisien, «l'EDI suppose [...] la transmission de données dans l'intention de produire des effets juridiques entre le système informatique d'une partie et celui d'un co-contractant[19].» Dans un système d'échange de données informatisées, l'authenticité, la sécurité, la confidentialité de même que l'intégrité des données sont assurées, notamment au moyen de la signature électronique.

La signature électronique, le *digital time-stamping* et le *hashing*

Pour être plus efficace, la cryptographie peut être combinée avec d'autres méthodes. Parmi celles-ci, la signature électronique est certainement la plus connue. Bien que son utilité première soit d'assurer l'authenticité du document auquel elle se rapporte, la signature électronique permet aussi de vérifier si un document a été ou non altéré entre le moment où il a été créé et signé par son créateur et le moment où il a été consulté. La signature électronique est généralement basée sur la cryptographie à clé publique. Une fois le document créé, il faut d'abord en réaliser un condensé au moyen d'une opération mathématique. Ensuite, ce condensé est encodé à l'aide de la clé secrète. C'est ce condensé encodé qui constitue la signature électronique. Celle-ci est donc réalisée à la fois à partir des données contenues dans le document et de l'utilisation d'une clé secrète. Par conséquent, elle permet de s'assurer que l'intégrité d'un document électronique ait été préservée, puisque si ce document est altéré, il devient indéchiffrable. Une telle méthode pourrait très bien être adaptée et appliquée à l'archivistique, en particulier pour la transmission de données sous forme électronique.

Un autre moyen qui mérite d'être souligné est ce qu'on appelle le *digital time-stamping*. Cette technique a été développée par Stuart Haver et Scott Stornetta. Il s'agit en quelque sorte d'un sceau électronique qui permet de connaître le moment où un document a été créé, de s'assurer que personne n'y a eu accès entre-temps et de vérifier s'il a été altéré ou non depuis. Comme c'était le cas pour la signature électronique, ce sceau électronique est créé à partir des données contenues dans le document.

Le *digital time-stamping* est généralement combiné avec une autre méthode appelée *hashing*, et plus particulièrement le *one-way hash function*. Elle consiste en des opérations mathématiques qui transforment de façon aléatoire toutes les chaînes

de caractères contenues dans le document en de plus courtes chaînes. Ce qu'on appelle le *hash value*, c'est-à-dire la valeur qui permet d'effectuer l'opération mathématique, peut être publiée et ne donne aucun indice sur la façon de décoder le document. Afin d'illustrer le fonctionnement de cette dernière méthode, nous reprenons ici l'exemple donné par Barry Cipra dans son article intitulé «Electronic Time-Stamping: The Notary Public Goes Digital»[20]. L'exercice consiste à convertir le mot *science* dans une chaîne de six chiffres. Pour commencer, on suppose que chacune des lettres est transformée en des séries de deux chiffres: a=01, b=02, etc. Ensuite, un chiffre est ajouté au début des séries de façon à décrire la position de chaque lettre dans le mot. Pour le mot *science*, on obtient les séries suivantes: 119, 203, 309, 405, 514, 603, 705. Puis, les nombres sont mis au carré et additionnés entre eux: $119^2 + 203^2 + 309^2 + 405^2 + 514^2 + 603^2 + 705^2 = 1439706$. Finalement, seuls les six derniers chiffres sont conservés, ce qui donne une valeur (un «*hash value*») de 439706. Comme on peut le constater, il suffit qu'un seul caractère contenu dans le document soit changé pour que la valeur soit complètement différente. Pour s'assurer que l'intégrité du document ait été préservée, le destinataire doit calculer le *hash value* du document. S'il est identique au *hash value* envoyé avec le document crypté, on peut avoir l'assurance que celui-ci n'a pas été altéré depuis le moment où le document a été signé et transmis.

Bien souvent, tous ces moyens plus «techniques» s'appliquent uniquement dans des contextes particuliers et ils offrent généralement des solutions partielles à la question de l'intégrité. Néanmoins, combinés entre eux, il peuvent assurément être très efficaces et être d'une grande utilité pour l'archiviste qui doit gérer des archives électroniques.

CONCLUSION

À un moment où les organisations créent et accumulent une quantité inquiétante et toujours croissante de documents sous forme électronique, les archivistes doivent rapidement trouver des solutions efficaces leur permettant d'assurer l'intégrité des données contenues dans les archives électroniques. Ces dernières années, des efforts ont été déployés et des progrès ont été réalisés dans ce domaine: le projet de recherche de la *University of Pittsburgh* et celui de la *University of British Columbia* en témoignent. Les modèles développés par chacun d'eux sont sensiblement différents. Le *Funtional Requirements for Evidence in Electronic Record-keeping Project* de la *University of Pittsburgh* propose notamment, nous l'avons vu, une série de conditions requises par un système de gestion de documents d'archives pour s'assurer que les archives électroniques demeurent intègres et conservent leur fonction de témoignage. Ces *functional requirements* reposent sur le *literary warrant* établi dans le cadre du projet, lequel consiste en un ensemble de lois, de normes et autres règles spécifiques dont la plupart sont issues de l'expérience américaine. Pour cette raison, les moyens mis de l'avant par ce projet pour résoudre la question de l'intégrité s'appliquent davantage au contexte nord-américain et pourraient être plus difficiles à implanter ailleurs dans le monde. Les solutions proposées par le *Preservation of the Integrity of Electronic Records Project* de la *University of British Columbia*, au contraire, sont davantage universelles et peuvent s'appliquer à des contextes plus divers. L'approche préconisée par le projet prend en considération le cycle de vie des archives et distingue les besoins des archives courantes et intermédiaires de ceux des archives définitives en ce qui concerne la préservation de leur intégrité.

Quoi qu'il en soit, les deux modèles ont chacun leurs forces et leurs faiblesses. Les différents projets pilotes qui ont été mis sur pied afin de les tester et de les évaluer montrent qu'ils sont plus ou moins bien applicables selon les milieux et qu'ils doivent être adaptés en fonction du contexte. Jusqu'à présent, les études n'ont pas démontré si l'un était plus valable que l'autre. Il est probable qu'aucun d'eux ne soit meilleur en soi et que des solutions encore plus efficaces puissent être trouvées en s'inspirant de chacun d'eux et en combinant certains des éléments qu'ils proposent. C'est notamment ce que pense Margaret Hedstrom: «Rather than selecting a single model, archivists and records managers would be better served by identifying which combination of policies, standards, system design methodologies, and implementation tactics are most effective for the particular organizational, business, technological, and cultural environments that they are trying to influence.[21]»

Bien que ces modèles apportent des solutions très intéressantes à la problématique des archives électroniques, les archivistes ont également tout intérêt à examiner et à prendre en considération certaines des solutions proposées à l'extérieur de la communauté archivistique. Nous avons vu certains moyens «techniques», développés principalement par des informaticiens et des mathématiciens, permettant à divers degrés d'assurer l'intégrité de documents électroniques: la cryptographie, la signature électronique, le *digital time-stamping* et le *hashing*. Une fois combinées, ces diverses solutions s'avèrent souvent très efficaces et pourraient assurément être mises à profit par les archivistes. Bien entendu, ces moyens doivent toutefois être envisagés avec prudence, puisque les technologies évoluent rapidement et qu'il est difficile de déterminer avec certitude lesquelles sont fiables et durables.

L'informatique et les mathématiques ne sont pas les seules disciplines à pouvoir venir en aide aux archivistes. En effet, ces derniers ont tout avantage à travailler en collaboration avec, par exemple, des avocats, des comptables ou d'autres professionnels de l'information. Fort heureusement, la communauté archivistique examine de plus en plus les progrès qui se font à l'extérieur de sa discipline et cherche à intégrer les solutions imaginées par d'autres pour résoudre des problèmes similaires. Cette ouverture aux autres disciplines est d'autant plus importante dans le cas des archives électroniques, l'informatique étant un domaine complexe et en constante et rapide évolution.

Taïk Bourhis Archiviste à la Sûreté du Québec.

NOTES

1. Couture, Carol. «Le concept de document d'archives à l'aube du troisième millénaire.» *Archives*, vol. 27, no 4, 1996. p. 6.
2. René-Bazin, Paule. «La création et la collecte des nouvelles archives». Actes du 11e Congrès international des Archives (Paris, 22-26 août 1988). *Archivum*, vol. XXXV, p. 47.
3. *Dictionnaire des archives : de l'archivage aux systèmes d'information*. AFNOR, 1991, p. 34.
4. Grimard, Jacques. «Gérer la préservation à long terme des archives électroniques ou préserver le médium et le message». *Archives*, vol. 27, nº 4, 1996, p. 22.
5. Marsden, Paul. «When is the Future? Comparative Notes on the Electronic Record-Keeping Projects of the University of Pittsburgh and the University of British Columbia.» *Archivaria*, vol. 43, Spring 1997, p. 159.
6. University of Pittsburgh. School of Information Sciences. *Production Rules Version of the Functional Requirements*. Page consultée le 24 janvier 1999. Adresse URL : http://www.sis.pitt.edu/~nhprc/IProdRule.html
7. *Ibidem*.

8. Duranti, Luciana et Heather *MacNeil*. «The protection of the integrity of electronic records : an overview of the UBC-MAS research project». *Archivaria*, vol. 42, Fall 1996, p. 46.
9. *Dictionnaire des archives : de l'archivage aux systèmes d'information*. AFNOR, 1991, p. 85.
10. Duranti, Luciana et Heather MacNeil. «The protection of the integrity of electronic records : an overview of the UBC-MAS research project». *Archivaria*, vol. 42, Fall 1996, p. 47.
11. *Ibid*. p. 49.
12. Duranti, Luciana. «Reliability and Authenticity : The Concepts and Their Implications». *Archivaria*, vol. 39, Spring 1995, p. 5-10.
13. University of British Columbia. School of Library, Archival and Information Studies (SLAIS). *The Preservation of the Integrity of Electronic Records*. Page consultée le 15 mai 1999. Adresse URL :

    http: / / www.slais.ubc.ca / users / duranti /
14. Duranti, Luciana. « Bâtir un avenir pour les documents électroniques : le projet InterPARES », *29e Congrès de l'Association des archivistes du Québec, Montréal, 1, 2, 3 juin 2000*.

    Pour obtenir plus d'informations sur le projet InterPARES : www.interpares.org
15. Hedstrom, Margaret. «Building Record-Keeping Systems : Archivists Are Not Alone on the Wild Frontier.» *Archivaria*, vol. 44, Fall 1997, p. 56-57.
16. *Dictionnaire des archives: de l'archivage aux systèmes d'information*. AFNOR, 1991, p. 75.
17. *Le Nouveau petit Robert*. Paris : Dictionnaires Le Robert, 1995, p. 56.
18. Schneier, Bruce. «Digital Signatures». *Byte*. November 1995, p. 310.
19. Parisien, Serge. «La sécurité dans le commerce électronique et l'échange de données informatisées». *Micro-gazette*, juin-juillet 1995, p. 15.
20. Cipra, Barry. «Electronic Time-Stamping : The Notary Public Goes Digital». *Science*, vol. 261, 9 July 1993, p. 162.
21. Hedstrom, Margaret. «Building Record-Keeping Systems : Archivists Are Not Alone on the Wild Frontier». *Archivaria*, vol. 44, Fall 1997, p. 63.

BIBLIOGRAPHIE

BERGERON, Pierrette. «La gestion des archives électroniques : quelques questions-clés à considérer». *Archives*, vol. 23, no 3, 1992, p. 51-70.

CIPRA, Barry. «Electronic Time-Stamping : The Notary Public Goes Digital». *Science*, vol. 261, 9 July 1993, p. 162-163.

COUTURE, Carol. «Le concept de document d'archives à l'aube du troisième millénaire». *Archives*, vol. 27, no 4, 1996, p. 3-19.

Dictionnaire des archives : de l'archivage aux systèmes d'information. AFNOR, 1991, p. 34, 75, 85.

DUFF, Wendy. «Ensuring the Preservation of Reliable Evidence : A Research Project Funded by the NHPRC». *Archivaria*, vol. 42, Fall 1996, p. 28-45.

DURANTI, Luciana. « Bâtir un avenir pour les documents électroniques: le projet InterPARES », *29e Congrès de l'Association des archivistes du Québec, Montréal, 1, 2, 3 juin 2000*.

DURANTI, Luciana. «Reliability and Authenticity: The Concepts and Their Implications». *Archivaria*, vol. 39, Spring 1995, p. 5-10.

DURANTI, Luciana et Heather MACNEIL. «The protection of the Integrity of Electronic Records : an Overview of the UBC-MAS Research Project». *Archivaria*, vol. 42, Fall 1996, p. 46-67.

GRIMARD, Jacques. «Gérer la préservation à long terme des archives électroniques ou préserver le médium et le message». *Archives*, vol. 27, no 4, 1996, p. 21-34.

HEDSTROM, Margaret. «Building Record-Keeping Systems : Archivists Are Not Alone on the Wild Frontier». *Archivaria*, vol.44, Fall 1997, p. 44-71.

MARSDEN, Paul. «When is the Future? Comparative Notes on the Electronic Record-Keeping Projects of the University of Pittsburgh and the University of British Columbia». *Archivaria*, vol. 43, p. 158-173.

PARISIEN, Serge. «La sécurité dans le commerce électronique et l'échange de données informatisées». *Micro-gazette*, juin-juillet 1995, p. 15-19.

POULTER, Alan. «Cryptography and records management». *Records Management Journal*, vol. 6, no 2, August 1996, p. 83-92.

RENÉ-BAZIN, Paule. «La création et la collecte des nouvelles archives». Actes du 11e Congrès international des Archives (Paris, 22-26 août 1988). *Archivum*, vol. XXXV, p. 47.

SCHNEIER, Bruce. «Digital Signatures». *Byte*, November 1993, p. 309-312.

UNIVERSITY OF BRITISH COLUMBIA. School of Library, Archival and Information Studies (SLAIS). *The Preservation of the Integrity of Electronic Records*. Page consultée le 15 mai 1999. Adresse URL : http: / / www.slais.ubc.ca / users / duranti /

UNIVERSITY OF PITTSBURGH. School of Information Sciences. *Functional Requirements for Evidence in Record-keeping*. Page consultée le 15 mai 1999. Adresse URL :..... http: / / www.sis.pitt.edu / nhprc /

ANNEXE 1

Functional Requirements for Evidence Within Record-Keeping

1. Compliant

ACCOUNTABLE RECORD-KEEPING SYSTEM

2. Responsible
3. Implemented
4. Consistent

CAPTURED RECORDS

5. Comprehensive
6. Identifiable
7. Complete
   - 7a. Accurate
   - 7b. Understandable
   - 7c. Meaningful
8. Authorized

MAINTAINED RECORDS

9. Preserved
   - 9a. Inviolate
   - 9b. Coherent
   - 9c. Auditable
10. Removable

USABLE RECORDS

11. Exportable
12. Accessible
    - 12a. Available
    - 12b. Renderable
    - 12c. Evidential
13. Redactable

Source: Duff, Wendy. «Ensuring the Preservation of Reliable Evidence : A Research Project Funded by the NHPRC.» *Archivaria*, vol. 42, Fall 1996, p. 41.

ANNEXE 2

University of Pittsburgh School of Information Sciences Project on the Functional Requirements for Evidence in Record-keeping

Literary Warrant Supporting Functional Requirements
Functional Requirements Ensuring Evidence in Record-keeping
Representing of the Functional Requirements in the form of Production Rules for Systems Development
Metada Specifications Enabling Business Acceptable Communications
Implementation in the Form of : Standards, Policies, Procedures, and Design

Source: University of Pittsburgh. School of Information Sciences. *Site Orientation*. Page consultée le 15 mai 1999. Adresse URL : http: / / www.sis.pitt.edu /~nhprc / orient.html

ANNEXE 3

Objectifs du projet de la *University of British Columbia*: *The Preservation of the Integrity of Electronic Records*

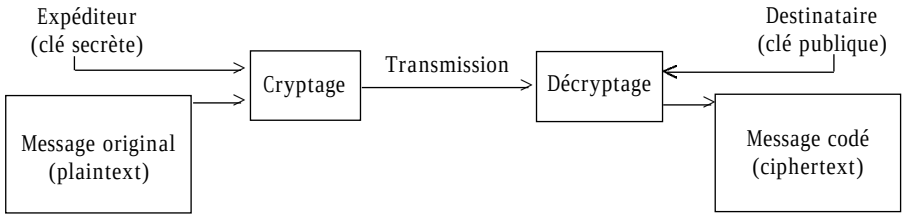
1. to establish what a record is in principle and how it can be recognized in an electronic environment ;
2. to determine what kind of electronic systems generate records ;
3. to formulate criteria that allow for the appropriate segregation of records from all other types of information in electronic systems generating and / or storing a variety of data aggregations ;
4. to define the conceptual requirements for guaranteeing the reliability and authenticity of records in electronic systems ;
5. to articulate the administrative, procedural, and technical methods for the implementation of those requirements ; and
6. to assess those methods against different administrative, juridical, cultural, and disciplinary points of view.

Source: Duranti, Luciana et Heather MacNeil. «The protection of the Integrity of Electronic Records : an Overview of the UBC-MAS Research Project». *Archivaria*, vol. 42, Fall 1996, p. 47.

ANNEXE 4

La cryptographie à clé publique

Pour assurer l'authenticité et l'intégrité d'un message:



Pour assurer la confidentialité d'un message: