La conservation de la signature électronique: Perspectives archivistiques

Rapport remis à la
Direction des Archives de France,
Ministère de la Culture

Jean-François Blanchette

Department of Information Studies
University of California, Los Angeles

Septembre 2004

Résumé

Depuis la Directive Européenne de 1999 et la réforme du droit de la preuve de 2000, l'écrit électronique signé est admissible et sa force probante reconnue en Droit français. Tant la Directive que le droit français ont consacré la supériorité des technologies de signature électronique fondées sur la cryptographie à clé publique, en leur reconnaissant une force probante particulière et une fiabilité exceptionelle.

L'obsolescence rapide qui caractérise les technologies de l'information, de même que l'extension de la réforme de 2000 aux actes authentiques électroniques, exige cependant que soit prise la pleine mesure des solutions techniques actuellement disponibles pour assurer la préservation de documents électroniques signés, de façon à ce que ceux-ci puissent remplir les fonctions attendues de la preuve documentaire.

Les solutions techniques actuellement disponibles — re-signature, préservation des équipements, émulation, canonicalisation — assimilent l'authenticité des documents à la simple préservation de l'intégrité physique de l'encodage binaire sous-tendant au document. De telles approches conservent la valeur de preuve des signatures cryptographiques, mais excluent les stratégies de préservation fondées sur la migration des formats logiques.

Les Archives Nationales des Etats-Unis, du Canada et de l'Australie ont publié des recommandations relatives au versement de documents électroniques signés. Ces recommandations témoignent de l'ambivalence de la communauté archivistique face à une technologie dont la préservation exige des ressources humaines et techniques considérables. La réflexion de la profession archivistique sur la signature électronique suggère que si celle-ci procure une sécurité incomparable à la transmission des documents dans l'*espace*, elle n'est pas adaptée à leur transmission authentique dans le *temps*.

Une preuve documentaire dont la complexité technique la met hors de portée de ses usagers et des professions chargées de l'administrer, ne remplit plus les objectifs de stabilité juridique et sociale envisagés par les rédacteurs du Code Civil. Il est donc essentiel que l'adaptation d'un outil aussi performant au contexte électronique implique l'ensemble des professions concernées par l'administration de la preuve documentaire — au premier chef, celle qui a charge de la préserver dans le temps.

Table des matières

1. Introduction*

L'Etat Français a engagé en l'an 2000 une réforme du droit de la preuve ayant pour objectif de pleinement reconnaître la valeur juridique des documents électroniques.[1] Cette réforme a été en partie initiée en réponse à une Directive Européenne de 1999 enjoignant l'ensemble des États Membres de reconnaître la force de preuve des signatures électroniques, en particulier celles fondées sur les technologies cryptographiques.[2,3] Cette Directive avait pour but d'établir le cadre juridique et régulatoire de services électroniques susceptibles d'agir comme moteur d'une société Européenne de l'information. En fait, comme le témoigne un marché demeuré relativement anémique,[4] la « dématérialisation » des transactions s'est avérée un processus beaucoup plus complexe que le simple déploiement d'infrastructures électroniques.

Une des plus importantes questions soulevées par la réforme de 2000 concerne la pérennité des écrits signés électroniquement. Cette question suppose de résoudre trois problématiques distinctes :

(1) La pérennité du *support* de l'écrit, c'est-à-dire les différents supports physiques susceptibles de recevoir de l'information numérique — rubans magnétiques, disques optiques, etc. ;

(2) La pérennité du *format d'encodage* de l'écrit, c'est-à-dire, le format utilisé pour encoder le document sous forme numérique — XML, TIFF, ou Word 2003 ;

(3) La pérennité des *technologies de sécurisation* de l'écrit, c'est-à-dire les différentes méthodes utilisées pour signer et assurer l'intégrité, de

---

* Coordonnées de l'auteur : Jean-François Blanchette, UCLA Department of Information Studies, GSEIS Bldg., Box 951520, Los Angeles, CA 90005-1520 ; Tél : +1 310 267 5137 ; Fax : +1 310 206 4460 ; Email : blanc@ucla.edu.

[1] « Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique », *Journal Officiel de la République Française,* 14 mars 2000, p. 3968.

[2] « Directive 1999/93/CE du Parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques », *Journal Officiel des Communautés Européennes,* 19 janvier 2000, L 13, p. 12.

[3] Dans ce rapport, on utilisera « signature électronique » pour désigner toute technologie électronique qui reproduit, d'une façon ou d'une autre, les fonctionnalités de la signature manuscrite, et « signature numérique » pour désigner plus particulièrement les technologies fondées sur la cryptographie à clé publique.

[4] Voir Morin, H. (2003), « Pourquoi la signature électronique reste lettre morte », *Le Monde* 22 juin 2003.

l'écrit, telle la signature numérique, l'horodatage, et le tatouage.

Si à ce jour, l'on dispose d'assez bonnes solutions pour la première de ces problématiques, et de certaines pistes pour la seconde, on comprend encore mal la troisième, et, plus important encore, on a peu considéré la question de résoudre ces trois problématiques *simultanément*.[5] Or le nouveau régime du droit de la preuve implique de pouvoir y répondre de façon exacte, puisque l'écrit électronique et sa signature numérique s'y trouvent désormais admissibles en justice et dotés d'une valeur probante. Il est donc essentiel de pouvoir concrètement déterminer les modalités de conservation de ce nouveau moyen de preuve.

Ce rapport, commandé par le Département de l'innovation technologique et de la normalisation de la Direction des Archives de France, prend la mesure des dimensions archivistiques de la réforme du droit de la preuve entamée depuis 2000. Pour ce faire, il décrit les technologies de signature numérique et le régime juridique qui les encadre depuis 2000, et articule de façon raisonnée et systématique le point de vue des archivistes sur ces technologies. Il analyse en détail les problèmes de conservation qui sont afférents à ces technologies, problèmes qui ne peuvent en aucun cas être réduits à de simples questions de taille de clés cryptographiques.

Après un résumé de la problématique en **section 1,** la **section 2** offre un survol de la signature numérique et des infrastructures nécessitées par son déploiement ; La **section 3** récapitule les principales étapes du développement d'un cadre juridique adapté à la reconnaissance de la valeur probante des signatures électroniques et numériques; La **section 4** décline les différentes solutions techniques proposées à ce jour visant à assurer la conservation des documents numériques signés; La **section 5** analyse les différentes approches proposées par la communauté archivistique pour permettre la conservation des documents numériques signés ; La **section 6** conclut en offrant un certain nombre de pistes et de recommandations susceptibles d'assister la Direction des Archives de France dans l'articulation de politiques et de normes relatives à la conservation de documents numériques signés.

---

[5] Voir Blanchette, J.-F. (2001), « Les Technologies de l'écrit électronique: Synthèse et évaluation critique », in *Les actes authentiques électroniques,* Paris, La Documentation Française.

2. Les technologies de signature numérique

Il convient de commencer par une brève description de la technologie de la signature numérique **(2.1)**, d'expliquer le principale de la certification **(2.2)**, et de brièvement décrire les infrastructures qui sous-tendent le déploiement des outils de signature dans les organisations **(2.3)**.

2.1 — Origine et contexte

Historiquement, la science des cryptologues a eu pour principale fonction de fournir aux Etats des moyens d'assurer la confidentialité des communications militaires ou diplomatiques. Ces moyens étaient, jusqu'en 1976, fondés sur un paradigme où l'émetteur et le récepteur d'une communication chiffrée se devaient de disposer d'une information commune, une *clé secrète*. Les problèmes relatifs au déploiement et à la mise en œuvre de systèmes de chiffrement se résumaient alors le plus souvent au problème de définir des procédures d'échange de clés qui soient elles-mêmes sécuritaires.

La science cryptographique, que Ronald Rivest définit comme celle de « la communication en présence d'adversaires »,[6] a connu un essor considérable depuis le début des années 70, alors qu'a été reconnue son utilité pour sécuriser les échanges bancaires.[7] C'est à cette occasion que la recherche fondamentale en ce domaine devait commencer à se dégager du cadre strictement militaire qui était jusqu'alors le sien. Elle connaîtra sa première heure de gloire en 1976, lorsque Whitffield Diffie et Martin Hellman conçoivent le principe de la cryptographie à clé publique et suggèrent que cet outil pourrait fournir un équivalent à la signature manuscrite au sein des environnements électroniques.[8]

Dans leur article, Diffie et Hellman proposent un mécanisme mathématique inédit permettant à deux individus d'échanger des données chiffrées, avec la propriété étonnante qu'*il ne nécessite pas de s'entendre au préalable sur une clé commune.* Ce mécanisme (désigné sous le nom de *cryptographie à clé publique*, ou *asymétrique*) procède d'un principe simple, mais très astucieux. À chaque

---

[6] Rivest, R. L. (1990), "Cryptography," in *Handbook of Theoretical Computer Science (Volume A: Algorithms and Complexity)*, Elsevier and MIT Press, p. 6.

[7] Un excellent exposé vulgarisé de la cryptographie moderne est celui de Stern, J. (1988), *La science du secret*, Odile Jacob ; pour des exposés plus historiques, voir Kahn, D. (1980) *La guerre des codes secrets : Des hiéroglyphes à l'ordinateur*, Inter Éditions ; Singh, S. (1999), *Histoire des codes secrets : De l'Égypte des pharaons à l'ordinateur quantique*, Lattès.

[8] Diffie, W. et Hellman, M. E. (1976), « New Directions in Cryptography », *IEEE Transactions on Information Theory*, IT-22, pp. 644-654.

individu présent au sein du réseau de communication, est attribuée une paire de clés, une *clé publique* et une *clé privée* (on parle parfois de bi-clés), qui permettent de réaliser et le chiffrement, et la signature. La clé publique de chaque individu est rendue disponible à tous et chacun au sein d'un annuaire, alors que la clé privée est conservée secrète. Toute la magie du système repose sur l'hypothèse mathématique suivante : *bien que la clé publique et la clé privée soient uniquement complémentaires, même en connaissant la clé publique, il est impossible (au sens calculatoire du terme) d'en déduire la clé privée*. Ce mécanisme permet d'échanger des données *chiffrées* et/ou *signées* :

- *Chiffrement :* Pour envoyer un message chiffré à Bernard, Alice obtient la clé publique de Bernard et s'en sert pour chiffrer le message. À sa réception, Bernard est en mesure de déchiffrer le message en utilisant sa clé privée. Nul autre que lui n'est en mesure de faire, puisque si n'importe qui peut accéder à la clé publique de Bernard, nul ne peut en déduire la clé privée qui la complémente;

- *Signature :* Pour envoyer un message signé, il suffit d'inverser l'ordre des clés : la clé privée devient la *clé de signature*, et la clé publique, celle de *vérification*. Le mécanisme offre alors les assurances suivantes : d'une part, le message ainsi « signé » l'a bel et bien été par la clé privée correspondant à la clé publique utilisée pour la vérification; d'autre part, le message n'a pu être modifié après la signature, sinon la vérification aurait échouée.[9] Ces deux caractéristiques —*identification* de l'auteur et *intégrité* du message signé — fournissent, selon Diffie et Hellman, un équivalent de la signature manuscrite adapté au contexte électronique.

Reste un problème de taille, la distribution des clés publiques. En effet, pour que le chiffrement et la signature fonctionnent, il faut pouvoir être certain de l'identité de *la personne reliée à la clé publique*. Pour ce faire, on utilise en général un procédé de *certification* des clés publiques.

2.2 — La certification

La solution de Diffie et Hellman souffre cependant d'une faiblesse importante, propre à invalider les bénéfices du système : supposons qu'Oscar, un être fourbe et malhonnête, désire convaincre Alice qu'elle reçoit des messages signés de Bernard, alors qu'ils sont en fait de la plume d'Oscar. Celui-ci n'aurait qu'à substituer sa propre clé publique à celle de Bernard dans l'annuaire, et envoyer ses messages à Alice en prétendant être Bernard. Pour vérifier la signature de ces messages, Alice se procurerait la clé publique de Bernard (en fait, celle d'Oscar) et la vérification étant réussie, serait faussement convaincue de l'origine des messages. Il faut donc que les clés publiques

[9] Pour plus de détails sur la signature cryptographique, voir Blanchette, *op. cit.*

soient obtenues de telle façon à ce que l'on puisse se convaincre de l'identité de la personne reliée à la clé.

La méthode la plus couramment utilisée consiste en l'utilisation d'un *certificat*, émis par une *autorité de certification*. Un certificat est tout simplement un document contenant une série d'informations permettant d'associer une clé publique à un individu. Par exemple, un certificat répondant aux exigences de l'annexe I de la Directive européenne sur la signature électronique pourrait ressembler à :

```
Nom                 :        Blanchette, Jean-François
Clé publique        :        AD3456EBE12976EDE
Date d'émission     :        01/01/2000
Date d'expiration   :        31/12/2004
Limite de valeur    :        1000 euros
Emis par            :        Direction Archives de France
Algorithme          :        DSA 1.78
Numéro de série     :        34343343434343433
Signature de l'AC   :        AB33838FB343BAA34
```

La véracité des informations contenues dans le certificat est confirmée par deux processus distincts :

(1) D'une part, l'autorité de certification engage une procédure par laquelle l'identité de la personne est confirmée — présentation en personne de pièces d'identités, etc. ;

(2) D'autre part, le certificat est lui-même signé électroniquement par la clé privée de l'autorité de certification.

Toute personne qui désire vérifier la véracité du lien entre un individu et sa clé publique peut dorénavant le faire, d'une part, en se procurant la clé publique de l'autorité de façon à pouvoir vérifier la signature de l'autorité de certification sur le certificat de l'individu et, d'autre part, en se convainquant, par tous les moyens à sa disposition, de la compétence de l'autorité de certification. Une fois muni de la clé publique d'une autorité de certification, un individu est en mesure de vérifier la signature des tous les signataires dont la clé publique a été dûment authentifiée par cette autorité.[10]

Par contre, il doit toujours être en mesure de se procurer la clé publique de

---

[10] Voir Ford et Baum (2000), *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*, Prentice Hall.

l'autorité de certification d'une façon sécuritaire — celle-ci étant vulnérable au même problème de substitution que le principe du certificat tente de résoudre. Plusieurs solutions à ce problème ont été proposées, mais le point le plus important à retenir ici est que la vérification d'une signature implique la vérification de la totalité de la *chaîne de certification*, c'est-à-dire l'ensemble des certificats des autorités de certification impliquées.

Un individu qui veut, aujourd'hui, obtenir un certificat à clé publique, peut le faire de différentes façons. Soit qu'il l'obtient d'une autorité de certification à partir du réseau. Ce certificat peut ensuite être intégré directement à son ordinateur (Windows 2000 supporte les certificats), soit que ce certificat est intégré à son logiciel de courriel ou à son fureteur Web, logiciels qui intègrent différentes fonctions de gestion de certificats.

2.3 — Les infrastructures à clés publiques

On utilise le terme *infrastructure à clés publiques* (ICP)[11] pour désigner la combinaison d'éléments matériels, logiciels, et procéduraux qui permette d'effectuer l'ensemble des opérations sous-jacentes à la réalisation de la signature (et du chiffrement) cryptographique, c'est-à-dire :

(1) *Génération de clés cryptographiques :* il faut produire les paires de clés cryptographiques, de façon hautement sécuritaire ;

(2) *Enregistrement des utilisateurs :* Il faut que l'autorité de certification vérifie l'identité de chacun des utilisateurs, par exemple par une présentation en personne de pièces d'identités ;

(3) *Certification des clés publiques :* Une fois l'identité des utilisateurs confirmée, l'autorité de certification doit produire le certificat et le signer avec sa clé privée ;

(4) *Distribution des clés privées aux utilisateurs :* il faut distribuer les clés privées aux utilisateurs, par exemple, en les plaçant au sein d'une carte à puce ;

(5) *Service d'annuaire :* Le certificat doit être placé au sein d'un annuaire, de façon à permettre à d'autres utilisateurs d'y accéder et de vérifier les signatures ;

(6) *Révocation des certificats compromis ou périmés :* Un service doit permettre de révoquer les certificats lorsqu'ils sont expirés, ou lorsqu'une clé privée a été compromise. Ainsi, à partir du moment où le certificat

[11] Ou encore, PKI pour *Public-Key Infrastructures*, ou IGC pour *Infrastructure de gestion de clés*.

d'une clé publique est révoqué, il ne peut être utlisé pour vérifier les messages signés à l'aide de la clé privée associée;

(7) *Archivage :* Il faut conserver l'ensemble des certificats qui permettent la vérification, les listes de révocation, etc., de façon à pouvoir effectuer la vérification ultérieurement ;

(8) *Recouvrement des clés :* Dans plusieurs pays, notamment la France, la Grande-Bretagne, et les Etats-Unis, les forces de l'ordre ont exprimé de grandes réserves face à l'impossibilité de pouvoir déchiffrer des messages qui circulent sur les réseaux. Les technologies de recouvrement de clés permettent, de différentes façons, d'accéder aux clés de chiffrement d'un utilisateur, ou encore, de récupérer les clés de déchiffrement si elles étaient égarées ;

(9) *Horodatage :* les certificats et les signatures doivent faire l'objet d'un datage sûr.

Une organisation désirant déployer une PKI peut déléguer l'ensemble de ces fonctions à un prestataire, ou au contraire, les réaliser toutes ou en partie. Cette liste permet cependant de constater d'un coup d'oeil la complexité des infrastructures nécessaires au déploiement de la signature cryptographique. Le coût afférent à ces infrastructures a considérablement freiné l'essor du marché de la PKI.[12]

2.4 — Conclusion

Les technologies de signature numérique, fondées sur la cryptographie à clé publique, nécessitent d'une part, le déploiement d'autorités de certification, chargées de délivrer les certificats qui lient l'identité d'un individu à sa clé publique et d'autre part, le déploiement d'infrastructures, les PKIs, qui assurent les fonctions de gestion de clés (révocation, renouvellement, etc.) nécessaires au fonctionnement du système de signature et/ou de chiffrement à clé publique.

Si l'invention de la cryptographie à clé publique a donné lieu à un essor scientifique remarquable, les conséquences *pratiques* de cette révolution sont nettement moins bien définies, et la cryptographie à clé publique demeurera, pendant les années 80 du moins, « une solution à la recherche d'un problème ». C'est l'explosion des technologies de l'Internet qui fournira, au milieu des années 1990, ce problème, c'est-à-dire la sécurisation du commerce électronique. La signature électronique, telle que proposée par Diffie et Hellman, va alors soudainement se retrouver au cœur d'une série d'initiatives

[12] Voir Morin, *op. cit.*

internationales visant à définir un cadre juridique pour les transactions électroniques.

3. Le cadre juridique de la signature numérique

À partir de 1996, la signature électronique, telle que proposée en 1976 par Diffie et Hellman, va se retrouver soudainement au cœur d'une série d'initiatives internationales visant à définir un cadre juridique pour les transactions électroniques. Supputant l'avènement prochain d'une société de l'information où tant les relations commerciales que les relations entre l'Etat et le citoyen seraient conduites par l'entremise de réseaux électroniques, l'*American Bar Association,* l'OCDE, et la CNUDCI publieront, respectivement, les *Digital Signature Guidelines*,[13] les *Cryptography Guidelines,*[14] la *Loi type sur le commerce électronique.*[15]

Ces documents offrent différentes approches à la définition d'un cadre juridique approprié à la reconnaissance de la valeur juridique de la signature électronique, certains se fondants sur des technologies particulières, d'autres demeurant le plus neutre possible. Le texte législatif le plus important à reconnaître un rôle particulier à la signature cryptographique demeure cependant la Directive Européenne du 13 décembre 1999 *« sur un cadre communautaire pour les signatures électroniques »*.[16]

3.1 — La Directive Européenne de 1999

Les Directives Européennes sont des instruments régulatoires très complexes, vu la diversité des objectifs qu'elles tentent d'accomplir — harmonisation des régimes juridiques, élimination des obstacles techniques au marché intérieur, couplage étroit régulation/standardisation. L'essentiel, en regard de ses implications pour le droit de la preuve, est la Directive de 1999 définit deux types de signature électroniques, et mande les Etats Membres de leur accorder une valeur juridique distincte. Le premier type, la signature électronique « simple », est défini comme

> « une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification. »[17]

alors qu'une signature électronique « avancée » est définie comme satisfaisant aux exigences suivantes:

> « (1) être liée uniquement au signataire; (2) permettre d'identifier le signataire; (3) être

---

[13] American Bar Association (1995), *Digital Signature Guidelines,* 1995.
[14] OECD (1996), « Cryptography Policy Guidelines, » OCDE/GD(97) 204.
[15] CNUDCI (1997), *Loi type sur le commerce électronique*.
[16] Directive, *op. cit*.
[17] Directive, *op. cit.* art. 2.1.

> créée par des moyens que le signataire puisse garder sous son contrôle exclusif; (4) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable; »[18]

En dépit d'une volonté de « neutralité technologique »,[19] cette définition est fondée, sans la nommer explicitement, sur le modèle de la signature cryptographique imaginé par Diffie et Hellman. En effet, l'exigence que la vérification de la signature échoue s'il y a modification, aussi infime soit-elle, des données du document suite à la signature est une des caractéristiques fondamentales de ce modèle.

À ces deux types de signatures électroniques correspondent deux régimes d'admissibilité et de force probante. Dans le cas d'une signature électronique « simple », la Directive exige des Etats Membres que ceux-ci se conforment au principe de « non-discrimination » énoncé par la CNUDCI,[20] c'est-à-dire que ceux-ci doivent veiller à ce que

> « … l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que … la signature se présente sous forme électronique … »[21]

Dans le cas des signatures électroniques « avancées », celles-ci sont non seulement admissibles, mais les Etats Membres doivent amender leurs droits nationaux respectifs de façon à ce qu'elles

> « répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier. »[22]

Ainsi, la Directive européenne impose aux Etats membres un régime probatoire où les signatures électroniques fondées sur les technologies de cryptographie à clé publique se voient accorder un statut préférentiel — valeur probante équivalente à celle d'une signature manuscrite — alors que les autres technologies sont regroupées en une catégorie de signatures électroniques dites « simples », admissibles, mais à la force probante indéterminée.

---

[18] *Ibid.*, art. 2.2.
[19] Récital 8 : « eu égard a la rapidité des progrès techniques et à la dimension mondiale d'Internet, il convient d'adopter une approche qui prenne en compte les diverses technologies et services permettant d'authentifier des données par la voie électronique. »
[20] CNUDCI, article 5 : « L'effet juridique, la validité ou la force exécutoire d'une information ne sont pas déniés au seul motif que cette information est sous forme d'un message de données. »
[21] Directive, *op. cit.*, art. 5.2.
[22] *Ibid.*, article 5.1.

3.2 — La réforme de 1980

La confrontation du droit de la preuve français au nouvelles manifestations de l'écrit a débuté avec la réforme de 1980,[23] occasion d'un examen du problème de la reconnaissance de la valeur probante d'écrits transmis à distance (télécopie), démultipliés (photocopie) et archivés sur support photographique (microfilm). Il faut souligner que ces nouvelles formes d'écrits posent à l'analyse doctrinale les mêmes défis conceptuels que ceux associés aux NTIC. Cependant, ils ne s'inscrivent pas dans une mouvance sociale comparable à celle si puissamment symbolisée aujourd'hui par l'Internet, et le législateur pourra alors se contenter de les soumettre à de simples régimes d'exceptions à l'exigence d'un écrit papier. En effet, l'article 1348 énonce que ces écrits

> « reçoivent … exception [à l'exigence de produire un original papier] lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction non seulement fidèle mais aussi durable. Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support. »[24]

Bien que la valeur probante de telles reproductions ne soient pas précisée, elles se voient accorder, en pratique du moins, la valeur d'original, puisque « la reproduction constitue un indice sérieux de l'existence antérieure du titre invoqué ».[25]

Si les objectifs pratiques de la réforme — au premier chef, apporter une solution aux problèmes d'archivage de plus en plus importants du secteur bancaire et des assurances — purent être atteints sans exiger une confrontation plus frontale de la doctrine aux nouvelles manifestations de l'écrit, une telle dérobade ne pouvait durer longtemps. Tout au cours des années 1980, des appels répétés se feront entendre pour que le droit positif prenne la pleine mesure des transformations induites par le déploiement des technologies de l'information et de la communication dans la vie quotidienne des citoyens.

3.3 — La réforme de 2000

Sensible à ces appels, le Ministère de la justice constituera en 1996 un groupe de travail, formé d'universitaires éminents,[26] avec pour mission de prendre la pleine mesure des nouvelles manifestations de l'écrit et de suggérer les paramètres d'une éventuelle réforme du droit de la preuve propre à actualiser

---

[23] Voir Vion, M. (1980), « Les modifications apportées au droit de la preuve par la loi du 12 juillet 1980 », *Desfrenois*.
[24] CC. art. 1348.
[25] Vion, *op. cit.*, 1334.
[26] Pierre Catala, Pierre-Yves Gautier, Jérome Huet, Isabelle de Lamberterie, Xavier Linant de Bellefonds, André Lucas, Lucas de Leyssac, et Michel Vivant.

les définitions du Code Civil relatives aux actes sous seing privé.

Le rapport du groupe, remis au Ministère en 1997, forma, en octobre 1998, la matière d'un avant-projet de loi « *relatif à l'adaptation du droit de la preuve aux nouvelles technologies* » puis d'un projet de loi déposé au Sénat en septembre 1999 et adopté à l'unanimité par l'Assemblée nationale le 29 février 2000.[27]

Quatre articles définissent à présent le cadre juridique de l'écrit électronique : tout d'abord, une définition de l'écrit où celui-ci est distingué de son support matériel:

> « La preuve littérale, ou preuve par écrit, résulte d 'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leur modalités de transmission. »[28]

Ensuite, une définition des règles selon lesquelles un écrit électronique peut être admis à titre de preuve, c'est-à-dire identification de son auteur et garanties quant à son intégrité:

> « L 'écrit sous forme électronique est admis en preuve au même titre que l 'écrit sur support papier, sous réserve que puisse être dûment identifié la personne dont il émane et qu 'il soit établi et conservé dans des conditions de nature à en garantir l 'intégrité. »[29]

Troisièmement, des instructions relatives à la manière de trancher en cas de conflit entre des écrits sur différents supports :

> « Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. »[30]

Finalement, une fois dûment qualifié, admis, et les conflits potentiels écartés, la loi définit la force probante d'un tel écrit:

> « L'écrit sur support électronique a la même force probante que l'écrit sur support

---

[27] Voir Catala et al. (1999), "L'introduction de la preuve électronique dans le Code civil," *La Semaine Juridique Édition Générale* **47**, pour une description et critique des différences entre l'avant-projet et le projet de loi.

[28] CC., art. 1316. Voir de Lamberterie, I. (1999) "L'écrit dans la société de l'information," in *Mélanges en l'honneur de Denis Tallon – D'ici, d'ailleurs: Harmonisation et dynamique du droit*, ed. Camille Jauffret-Spinosi and Isabelle de Lamberterie (Paris: Société de législation comparée); ainsi que de Lamberterie, I. (2000), "Preuve et Signature: Les innovations du droit français," *Cahiers Lamy droit de l'informatique et des réseaux* K, no. 123.

[29] CC. art. 1316-1.

[30] CC. art. 1316-2.

papier. »[31]

Bien sûr, pour que ces règles puissent constituer un cadre cohérent et complet à même de pouvoir tenir compte de l'ensemble des règles relatives aux actes sous seing privé, il manque l'élément essentiel de la signature. Bien que le rapport original des universitaires ne discute pas du problème d'une signature adaptée au contexte de l'écrit électronique, une définition de celle-ci fait son apparition dans l'avant-projet de loi et émergera largement intacte du processus de réécriture du texte de loi opéré par le Ministère suite à la circulation de l'avant-projet.

La loi de 2000 commence par définir les fonctions attendues d'une signature — que celle-ci soit manuscrite ou électronique — c'est-à-dire identification et manifestation du consentement:

> « La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. »[32]

Elle définit ensuite, au second alinéa de l'article 1316-4 un *objet informatique*, la signature électronique, à même de reproduire les fonctions d'une signature au sein des environnements électroniques: celle-ci doit pouvoir *identifier* le signataire; elle doit pouvoir être, d'une façon ou d'une autre, *liée* à l'acte auquel elle se rapporte; et ces fonctions doivent être assurées par le procédé de signature d'une façon *fiable* :

> « Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. » [33]

La deuxième partie du second alinéa de l'article 1316-4 introduit un mécanisme qui permette de spécifier les conditions selon lesquelles un tel procédé ne sera pas simplement *considéré*, mais plutôt, *présumé*, fiable :

> « La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'état. »[34]

Ce décret, publié en mars 2001, fournit le mécanisme par lequel le droit de la preuve français s'est rendu conforme aux exigences de la Directive européenne.

---

[31] CC. art. 1316-3.
[32] CC. art. 1316-4, premier alinéa.
[33] CC. art. 1316-4, second alinéa.
[34] CC. art. 1316-4, second alinéa.

3.4 — La transposition de la Directive en droit français

La jonction entre les exigences de la Directive et le processus amorcé au sein du système juridique français allait s'effectuer au sein d'un groupe de travail constitué par le Conseil d'état à la requête du Premier Ministre, et chargé « d'analyser les questions juridiques liées au développement d'Internet et de mettre en lumière les adaptations nécessaires de notre droit. »[35] Le groupe de travail allait énoncer un parti pris clair pour les technologies de signature basées sur la cryptographie, supputant sa généralisation prochaine :

> « En pratique, les signatures électroniques sont aujourd'hui rendues fiables par un recours à des techniques cryptographiques similaires à celles utilisées pour le chiffrement. Parmi celles-ci, le procédé dit de la « signature numérique à clé publique » est sans doute le mieux adapté à la signature de messages électronique et tout laisse penser que son usage devrait rapidement se généraliser au niveau mondial. Ce procédé permet de signer des messages électroniques dont l'origine et l'intégrité sont certifiées par un tiers dit de certification. »[36]

Face à des technologies aussi complexes, la délicate question de l'équilibre de la charge de la preuve devient prépondérante. En effet, comment un individu qui conteste la validité d'une signature peut-il faire la preuve de ce qu'il avance, et comment le juge peut-il apprécier la validité d'une telle contestation ? Le Conseil allait estimer qu'

> « en conformité avec le projet de directive sur la signature électronique, il convient d'admettre qu'un document électronique certifié par un tiers dûment accrédité conduit à présumer satisfaites les exigences légales. »[37]

C'est le Conseil qui allait introduire la notion de présomption légale de fiabilité (par ailleurs nulle part exigée par la Directive), présomption fondée sur un désir d'établir un équilibre dans le fardeau de la preuve, mais également, sur les qualités techniques exceptionnelles accordées à la signature cryptographique: ne convient-il pas que celui qui doute des qualités d'un moyen de preuve aussi performant soit chargé d'étayer ce doute?

Cette présomption est accordée lorsque le procédé de signature établit sa conformité à « des conditions fixées par décret en Conseil d'état, » décret promulgué le 30 mars 2001.[38] Si on a reproché à ce décret une architecture baroque qui met à mal un droit de la preuve aux lignes élégantes et patinées par le temps, il n'est pourtant rien de plus que la transcription des définitions et des annexes de la Directive Européenne de 1999. Sa logique culmine à l'article 2, qui énonce que toute signature fondée sur les principes de la

---

[35] Conseil d'État (1998), *Internet et les réseaux numériques*, La Documentation Française.
[36] *Ibid.*, p. 57.
[37] *Ibid.*, p. 56.
[38] CC. art. 1316-4, second alinéa.

cryptographie à clé publique se verra accorder une présomption de fiabilité:

> « La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve du contraire lorsque ce procédé met en oeuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d 'un certificat électronique qualifié. »[39]

Ainsi, la nécessité de concilier, d'une part, la réflexion des juristes français, centrée sur le problème de la reconnaissance juridique d'un « écrit électronique », et d'autre part, l'emphase de la Directive sur la seule question de la signature, en particulier la signature cryptographique, aboutit en un régime du droit de la preuve à la cohérence incertaine.

3.5 — Les actes authentiques électroniques

La réforme 2000 ne couvre pas uniquement le champ des actes sous seing privé. Elle s'est aussi préoccupée de l'acte authentique, sommet de la hiérarchie probatoire du droit français, et regroupant notamment les minutes notariales, les minutes des jugements, les actes de l'état civil et certains actes d'huissiers (notamment les significations). L'acte authentique acquiert sa force probante exceptionnelle en raison de la qualité de celui qui le confectionne (un officier public) et des solennités qui entourent son établissement. Sa définition a elle aussi été remaniée de façon à tenir compte de sa manifestation potentielle sous forme électronique. Ainsi, le vénérable article 1317 du Code Civil se lit à présent :

> « L'acte authentique est celui qui a été reçu par des officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises. Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat. »[40]

Alors que la signature ne formait auparavant qu'une des nombreuses formalités nécessaires à l'authenticité de l'acte, la réforme de 2000 a accentué l'importance de la signature, en ajoutant à l'article 1316-4 que

> « Quand [la signature] est apposée par un officier public, elle confère l'authenticité à l'acte ».[41]

Cependant, si la réforme inscrit sans ambiguïté le concept d'acte authentique électronique dans le droit de la preuve français, elle renvoie la définition de ses conditions matérielles à un décret d'application. À ce jour, deux groupes distincts, tous deux mandés par le Ministère de la Justice de fournir les

---

[39] *Ibid*.
[40] CC., article 1317.
[41] CC., article 1316-4.

éléments d'un tel décret d'application, n'ont pu éviter de constater l'extrême complexité de la question. Malgré l'enthousiasme initial avec lequel certaines des professions de l'authenticité ont épousé ces avancées technologiques,[42] le rapport du premier groupe de travail note que :

> « le décret fixant les conditions d'établissement et de conservation de l'acte authentique doit pouvoir rendre indépendante la signature électronique de l'usage de tout procédé de sécurité dont la conservation à long terme est hypothétique ». [43]

Aujourd'hui, plus de quatre ans après la réforme de 2000, les conditions matérielles de l'établissement, de la signature et de la conservation de l'acte authentique restent toujours à définir par le biais d'un décret en Conseil d'État. Le problème de la conservation à long terme de la signature électronique pose un obstacle particulièrement important à la rédaction de ce décret.

3.6 — Conclusion

Ainsi, le tableau final de l'écrit électronique dans le droit de la preuve français est le suivant :

- L'écrit électronique est défini et admis, avec une force probante équivalente à celle de l'écrit sur support papier, en autant que l'identité de son auteur et une conservation compétente, garantissant son intégrité, soit assurée (CC. Art. 1316) ;

- Une technologie particulière de signature électronique, celle fondée sur la cryptographie asymétrique, bénéficie d'une présomption de fiabilité (CC. Art. 1316-4 et décret du 30 mars). Bien que tout procédé de signature électronique répondant à la définition de 1316-4 soit admissible, le mode de démonstration de la fiabilité de ces procédés n'est pas spécifié ;

- La signature cryptographique assure également l'intégrité de l'écrit, puisqu'elle est « liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable » : Cependant, la coordination de cette exigence avec l'article 1316-2 n'est nulle part précisée;

- Les faiblesses de la Directive se retrouvent à l'identique dans le décret

---

[42] Voir par exemple Leclercq, P. (2000). « Rapport de synthèse: Vers l'authenticité électronique, Dixièmes Rencontres notariat-université », *Les Petites Affiches* **390**(65): 35–39; UINL (2000). *Les nouvelles technologies informatiques et l'acte authentique.*

[43] De Lamberterie, I. (2001), *Les actes authentiques électroniques. Réflexion Juridique Prospective.* La Documentation Française, p. 86.

du 30 mars qui la transpose, c'est-à-dire que le processus de vérification n'est nullement régulé,[44] et que la conservation dans le temps des signatures cryptographiques n'est nulle part abordée[45] (décret du 30 mars) ;

- Le principe d'un « acte authentique électronique » est défini par le Code Civil, mais le décret spécifiant les conditions de sa réalisation concrète peut difficilement être complété tant que des solutions concrètes au problème de la préservation des documents électroniques signés ne sont pas apportées.

[44] De Lamberterie, I. et Blanchette, J.-F. (2001), « Le décret du 30 mars relatif à la signature électronique: Lecture critique, technique et juridique », *La Semaine Juridique --- Entreprises et affaires*, no. 30.
[45] Blanchette, *op. cit*.

4. Approches techniques à la conservation de la signature numérique

L'écrit électronique est archivé de façon à ce qu'on puisse, d'une part, l'*exploiter* (production de copies conformes, etc.), et d'autre part, *démontrer* qu'il est authentique,[46] dans l'éventualité d'une opposition à cet écrit. En d'autres termes, on veut pouvoir non seulement accéder au contenu informationnel de l'écrit, mais également déterminer son auteur et démontrer son intégrité à un juge dans le cadre d'un contentieux. Un écrit prétendant servir comme preuve documentaire doit nécessairement pouvoir fonctionner simultanément sur ces deux registres.

Dans le contexte du cadre juridique proposé par la Directive, la démonstration de l'authenticité de l'écrit électronique ne peut prendre qu'une seule forme: *vérifier que la signature électronique apposée sur le document est belle et bien valide*.

Cette exigence est cependant problématique si l'on considère la figure 1, représentant la ligne de vie d'une signature électronique et les quatre étapes distinctes qu'elle est susceptible de traverser:

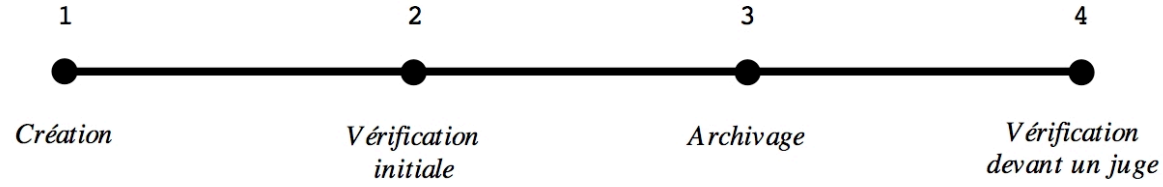

Figure 1: La ligne de vie d'une signature électronique

Au moment (1), la signature est créée par le signataire. Celui-ci l'envoie au destinataire, qui (2) effectue les vérifications nécessaires pour s'assurer de la validité de la signature — nous reviendrons plus tard sur la forme exacte de ces vérifications. Si le processus de validation réussit, le document est (3) archivé de même que la signature électronique, dans l'éventualité d'une contestation qui nécessiterait que (4) la signature sur le document soit vérifiée de nouveau devant un juge. Évidemment, la phase (4) est rarissime, mais la finalité du processus d'archivage est néanmoins de pouvoir réaliser correctement cette opération si elle doit avoir lieu.

---

[46] On entend ici « authentique » au sens archivistique du terme, et non au sens du droit civil français.

Ce diagramme met en évidence un aspect important mais longtemps négligé du processus de la signature électronique : si les vérifications effectuées en (2) et (4) sont conceptuellement identiques, elles sont cependant nécessairement séparées par le laps de temps plus ou moins grand qui intervient entre la création d'un document et son utilisation dans le contexte d'un contentieux. Ces laps de temps sont généralement bornés par les délais de prescription propres aux différentes catégories d'actes juridiques — souvent trentenaires dans le domaine civil, illimités dans le cas des actes authentiques.

Or, dans le contexte de documents électroniques, de tels laps de temps sont nécessairement caractérisés par l'obsolescence rapide associée aux technologies de l'information. Equipements matériels, logiciels et formats de données subissent sans relâche les effets de cycles d'innovation technologique et développement industriel toujours plus rapides.

Malgré ce phénomène d'obsolescence, au moment (4) du cycle de vie de la signature électronique, on doit pouvoir disposer d'un document dont le contenu soit intelligible, c'est-à-dire qu'on dispose d'équipements qui puissent accéder à la représentation binaire du document sur son support physique, la décoder, et rendre le document manifeste, sur écran ou sur papier. De même, on doit pouvoir disposer d'équipements qui puissent rendre la signature électronique intelligible, ce qui implique de pouvoir accéder à la signature électronique sur son support physique, de la décoder et d'exécuter l'algorithme de vérification qui permet de déterminer la validité de la signature.

Dans le contexte de la signature cryptographique, il existe cependant une relation étroite entre la capacité de préserver l'intelligibilité du document et celle de préserver l'intelligibilité de la signature. En effet, une des caractéristiques fondamentales de la signature cryptographique est que toute modification à l'intégrité logique d'un document signé cryptographiquement, *même d'un seul bit*, entraîne l'échec de la vérification. Ceci permet d'obtenir la certitude qu'un document n'a pu être modifié après sa signature sans que cette modification ne soit détectée au moment de la vérification.

Or, en pratique, la préservation de l'intelligibilité des documents électroniques est assurée par une migration de leur format d'encodage logique, de façon à ce qu'il demeure en phase avec les équipements logiciels et matériels permettant de décoder et rendre manifeste le document.[47] Une telle

---

[47] Pour une présentation synthétique des aspects techniques du problème de la préservation des objets numériques, voir Thibodeau, K. (2002). *Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years*, *in* The State of Digital Preservation: An International Perspective, Washington D.C., Council on Library and Information Ressources.

pratique invalidera nécessairement les signatures apposés sur les documents, l'algorithme de vérification ne faisant aucune distinction entre les modifications effectuées par un archiviste en vue d'assurer l'intelligibilité du document, et celle effectuées dans une intention malhonnête.

Il en ressort que l'archiviste qui est chargé d'assurer la préservation de documents signés cryptographiquement doit accomplir deux missions technologiquement incompatibles :

- D'une part, assurer l'intelligibilité du document nécessite des modifications à son format logique qui invalide automatiquement la signature cryptographique associée ;

- D'autre part, assurer l'intelligibilité des signatures nécessite de préserver l'intégrité logique des documents, c'est-à-dire des chaînes de bits qui les sous-tendent. Sur le long terme, ces documents deviennent fonctionnellement illisibles, alors que les équipements logiciels et matériels permettant de les décoder disparaissent.

Les sections qui suivent recensent les solutions actuellement proposées pour la conservation à long terme de documents électroniques signés — la re-signature **(4.1)**, l'émulation **(4.2)**, et la canonicalisation **(4.3)**.

4.1 — La re-signature

Une solution à la pérennisation des procédés cryptographiques de signature est couramment mentionnée, celle de la *re-signature*. Le consortium européen de standardisation de la signature électronique EESSI *(European Electronic Signature Standardization Initiative)*, se fonde sur cette approche.[48]

La sécurité d'un procédé cryptographique se détermine en partie à partir de la taille des clés utilisées: pour rendre un système cryptographique plus sécuritaire, il suffit d'augmenter la taille de la clé utilisée, avec le désavantage d'impacter négativement la rapidité du système. Quelle taille de clés faut-il alors utiliser de façon à conjuguer sécurité et performance, et pour combien de temps une telle clé procure-t-elle une sécurité suffisante ? La recherche d'une réponse à ces questions a donné naissance à une petite industrie académique parallèle : l'amélioration des algorithmes qui permettent de casser les procédés de cryptographie à clé publique.[49]

---

[48] Voir http://www.ict.etsi.org/eessi/EESSI-homepage.htm.

[49] Le dernier record est la factorisation d'un nombre de RSA de 512 bits — voir Cavalar, Dodson, Lenstra, et al., « Factorization of a 512-Bit RSA Modulus » in *Advances in Cryptology — EUROCRYPT 2000*, LNCS 1807, Springer 2000, pp. 1-17.

Ainsi, la sécurité procurée par la cryptographie diminue avec le temps, et il est loin d'être simple d'évaluer avec précision le *taux de cette diminution*.[50] Un message pouvant être chiffré en toute confiance avec une clé de *n* bits au temps *t* pourra être déchiffré au temps *t* + *x* années — et similairement pour un message signé cryptographiquement. Ceci est problématique car si l'écart entre les moments (2) et (4) de la figure 1 est suffisamment grand, alors la vérification devant le juge ne pourra être valide, car l'assise fondamentale de la sécurité cryptographique sera faussée par la possibilité que la taille des clés initialement utilisée soit désormais insuffisante.

La figure 2 reproduit ci-dessous le processus de validation du format de signature *ES-A (Electronic Signature – Archive Validation Data)*, un format développé par EESSI dans le but de « permettre la vérification de la signature longtemps après sa création. »[51] Dans le contexte de la ligne de vie d'une signature électronique (figure 1), le processus représenté à la figure 2 correspond à la validation effectuée au moment (2), dans le but de former un objet qui puisse être utilisé dans une validation au moment (4).

Puisque le modèle de la signature cryptographique suppose que *la vérification* de la signature est le seul moyen de s'assurer qu'une signature est valide, on doit obtenir toutes les composantes qui forment la signature cryptographique et les fournir à l'algorithme de validation pour obtenir la réponse `signature valide/invalide`.

---

[50] Lors de la présentation du système RSA dans les pages du *Scientific American* d'août 1977, les auteurs offrirent un prix de 100 dollars à quiconque réussirait à déchiffrer un message chiffré à l'aide d'une clé de 425 bits, prédisant qu'un tel exploit nécessiterait des milliards d'années de calcul sur ordinateur. Or, le contenu de ce message *(« and the magic words are squeamish ossifrage »)* fut déchiffré le 27 avril 1994, moins de 20 ans après la publication du défi — voir http://www.math.okstate.edu/~wrightd/numthry/rsa129.html.

[51] EESSI (2002), *Electronic Signature Formats*, ETSI TS 101 733 V1.2.2 (2000-12).

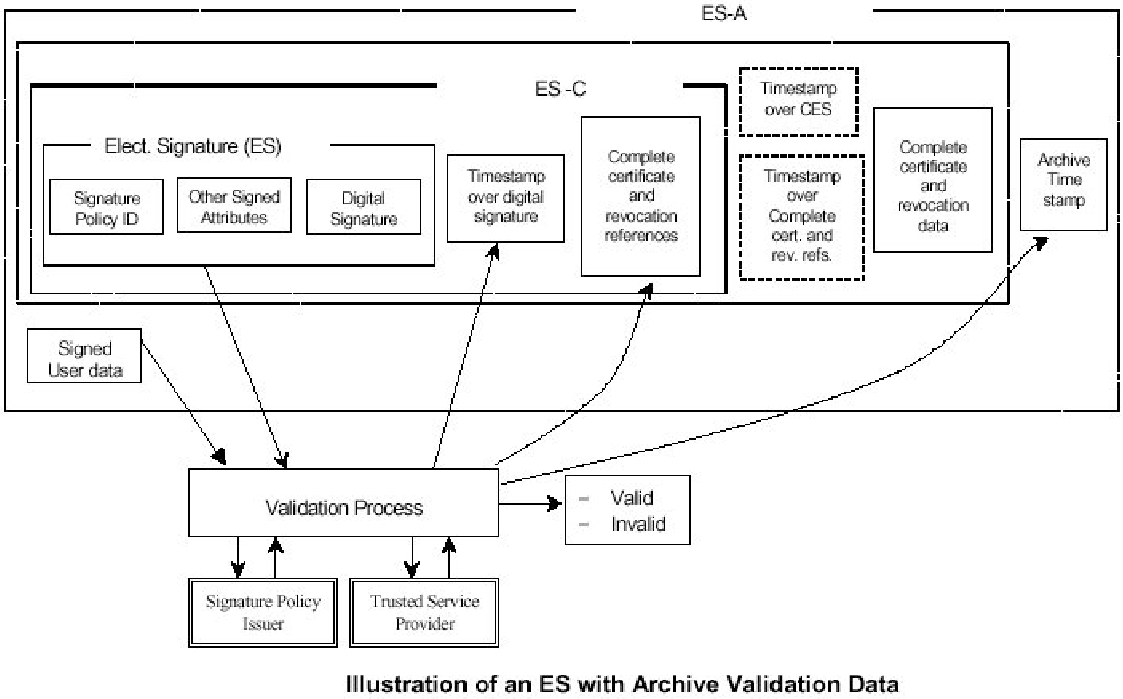

Figure 2: Validation du format de signature électronique ES-A — tiré de « Electronic signatures formats » ETSI TS 101 733 V1.2.2 (2000-12).

Le processus de validation implique six éléments principaux : (1) le rectangle intérieur marqué *ES* ; (2) un algorithme de validation (rectangle marqué *Validation Process*) — qui reçoit en entrée les éléments de (1) et interagit avec (3) l'émetteur de la politique de signature *(Signature Policy Issuer)* et (4) des fournisseurs de service de confiance *(Trusted Service Provider)* pour finalement émettre en sortie une réponse (5) : la signature est valide ou n'est pas valide ; si la signature est valide, alors le processus produit (6) les éléments du rectangle supérieur (marqué *ES-A*), c'est-à-dire l'ensemble des éléments de la signature archivée.

Le processus technique est le suivant : tout d'abord, le processus réalise la validation initiale (moment (2) de la ligne de vie), ce qui implique, dans l'ordre, de :

(1) Obtenir le certificat à clé publique du signataire d'une des Autorités de confiance *(Trusted Service Provider)* ; obtenir le certificat à clé publique de l'Autorité de certification qui a signé le certificat du signataire ; si nécessaire, obtenir le certificat à clé publique de l'Autorité de certification qui a signé le certificat de la première Autorité de certification ; répéter jusqu'à l'obtention d'un certificat-racine ;

(2) Vérifier sur les listes de révocation relatives à chacun de ces certificats si le certificat a été révoqué. Si oui, la signature est invalide ; si non,

vérifier, pour chacun des certificats, s'il a été suspendu ; si oui, attendre jusqu'à la fin de la période de suspension du certificat et reprendre le processus à l'étape **1**;

(3) Vérifier chacune des signatures sur les certificats, dans l'ordre du chemin de certification, en partant du certificat-racine ; si l'une de ces signatures est invalide, alors la signature est invalide ;

(4) Calculer, à l'aide de la fonction de hachage spécifiée dans la Politique de signature *(Signature policy)*, le condensé du document qui est l'objet de la signature *(Signed User data)*;

(5) Appliquer la clé publique contenue dans le certificat à clé publique du signataire au condensé calculé à l'étape précédente ; si le résultat est identique à la signature numérique (*Digital Signature*, troisième élément du rectangle ES), la signature est valide, sinon elle est invalide ;

Ensuite, le processus de validation construit l'objet qui pourra servir au moment (4), ce qui implique, dans l'ordre, de :

(1) Horodater la signature numérique (bloc marqué *digital signature*) de façon à lui donner une date, date qui permettra d'établir l'existence de la signature relative aux listes de révocations et à la période de validité des certificats ; ajouter les références complètes à tous les certificats utilisés de même qu'aux informations de révocation — l'objet résultant a pour nom *ES-C* ;

(2) Horodater le bloc *ES-C* ; horodater les références aux certificats et aux informations de révocation ; ajouter les certificats eux-mêmes et les données de révocation ; ajouter le document original, objet de la signature ;

(3) Horodater le tout — l'objet résultant est une signature de format *ES-A* ;

(4) Répéter l'étape précédente à chaque fois que la taille des clés ou la force des algorithmes utilisés par l'Autorité d'horodatage n'est plus jugée suffisante.

Il faudra ajouter aux vérifications mentionnées ci-dessus la vérification de chacun des horodatages. En effet, dans le modèle EESSI, l'horodatage d'un document par une Autorité d'horodatage s'effectue en deux opérations simples : (a) ajouter au document une date et une heure obtenue d'une source fiable et (b), signer le tout avec la clé privée de l'Autorité. Ces horodatages sont donc en fait des signatures supplémentaires pour lesquelles on devra

également vérifier la chaîne de certification.[52]

Ainsi, la re-signature, telle que proposée par l'EESSI pose comme principe que, dans le contexte de la ligne de vie de la signature, le moment (4) de vérification devant le juge doit correspondre en tout point au moment (2), c'est-à-dire que *le juge doit être en mesure de répéter la même expérience qui a eu lieu lors de la vérification initiale*. Le problème de la préservation de la valeur de preuve des documents signés est abordé sous le seul angle de la force des clés cryptographiques appliquées au document et de la diminution de leur performance dans le temps.

4.2 — L'émulation

Le consortium EESSI a également commandé une étude préliminaire sur les fonctions et caractéristiques d' « opérateurs fiables de services d'archivage » (*Trusted Archival Services*), partant de l'hypothèse que « des services centralisés d'archivage pourraient jouer un rôle important dans le support de signatures électroniques devant être utilisées comme preuve longtemps après leur création ».[53] L'étude propose une liste de quatre exigences techniques *(technical requirements)* que devraient rencontrer de tels opérateurs fiables de services d'archivage:

(1) *Encodage des documents*: les opérateurs doivent être en mesure d'identifier un certain nombre de formats de documents qu'ils s'engagent à préserver — par exemple PDF, TIFF, ou XML;

(2) *Interopérabilité*: les opérateurs doivent être en mesure de préserver de multiples formats de signatures — par exemple, RSA, DSA, ou autre;

(3) *Suivi cryptographique*: les opérateurs doivent être en mesure de régulièrement évaluer le statut des algorithmes cryptographiques, leur vulnérabilité et la taille des clés nécessaires pour en assurer la sécurité;

(4) *Compatibilité rétroactive*: les opérateurs doivent être en mesure de préserver les *logiciels originaux* de lecture et de signature, ou d'offrir des logiciels permettant de les émuler;[54]

---

[52] Il faut souligner que le cas présenté est celui d'un document signé par une seule personne. La solution proposée ne traite pas des signatures multiples sur un même document, où chacune des signatures dépend de leur propre chaîne de certification.

[53] Voir Libon, O., Mitrakas, A., *et al.*, (2000), *Trusted Archival Services*, disponible à http://www.law.kuleuven.ac.be/icri/publications/91TAS-Report.pdf?where=, p. 2 ;

[54] « Les opérateurs doivent maintenir un ensemble d'applications (logiciels de visualisation, de même que les logiciels de validation de signature), de même que les plateformes informatiques correspondantes (matériel, systèmes d'opération, etc), ou au moins la capacité

Ainsi, face au problème de l'obsolescence technologique qui frappera inexorablement les données dont ils auront la charge, cette dernière exigence suggère que les opérateurs fiables de services d'archivage préservent leur capacité à lire les documents et à vérifier les signatures sur ces documents de deux façons :

(1) Soit en préservant les équipements originaux, c'est-à-dire l'ensemble des logiciels, des plates-formes informatiques, et des équipements matériels qui permettent de visualiser les documents et de vérifier la validité des signatures sur ces documents ;

(2) Soit en utilisant des technologies permettant d'*émuler* ces équipements, c'est-à-dire qui permettant de récréer sous forme purement logicielle l'environnement informatique original, incluant ses éléments matériels et de réseau.[55]

Dans les deux cas, l'intégrité du document original et de sa signature sont parfaitement préservée, et ce sont les instruments de lecture et de vérification qui devront êtres maintenus utilisables au temps présent.

4.3 — La canonicalisation

Le concept de « format canonique » a été proposé par Lynch en 1999 comme méthode de préservation pour l'information numérique.[56] Il consiste en la migration d'un fichier de données encodé dans un format de données quelconque vers un format qu'on se sent plus confiant de pouvoir préserver. Ainsi, un document encodé dans un format de traitement de texte quelconque (p.ex., Word 2003) peut toujours être sauvegardé en format « Texte », avec l'inconvénient de faire disparaître la totalité des informations stylistiques (police et taille de caractères, notes de renvoi, etc.).

Cette approche est utilisée par le consortium W3C (responsable du développement du format XML), dans le cadre d'activités visant l'intégration des signatures cryptographiques au langage XML.[57] Une spécification du

---

d'émuler de tels logiciels et/ou environnements informatiques, **de façon à garantir que le contenu des documents puisse toujours être lu et que la signature sur ces documents puisse toujours être validé plusieurs années plus tard** », *idem,* p. 31.

[55] Cette approche, proposée comme technologie de préservation numérique en 1995 par Rothenberg, est celle qui sous-tend les logiciels comme VirtualPC, permettant de reproduire les fonctionnalités de la plateforme Windows au sein d'un environnement Macintosh. Voir Rothenberg, J. (1995), « Ensuring the Longevity of Digital Documents », *Scientific American* **272**(1): 24–29.

[56] Lynch, C. (1999) « Canonicalization: A Fundamental Tool to Facilitate Preservation and Management of Digital Information », *D-Lib Magazine* **5**(9).

[57] Cette approche est également utilisée par le format S/MIME pour les courriels signés.

langage XML dite « canonique »[58] a pour objet de définir :

> « une méthode pour exprimer la structure d'un document XML de façon univoque, éliminant ainsi tout désaccord de syntaxe possible […]. **Cette fonctionnalité est nécessaire pour les signatures XML qui requièrent des documents logiquement structurés dans le traitement de signatures électroniques, pour que d'éventuelles incompatibilités ne puissent pas invalider la signature** ».[59]

En d'autres termes, un document XML signé peut subir, au cours d'un traitement quelconque, des changements de forme sémantiquement insignifiants, mais qui le modifie et invalide ainsi la signature cryptographique associée. Le format XML canonique effectue ainsi un prétraitement sur le document *avant qu'il soit signé*, dans le but d'éliminer autant que possible ces changements de forme. Par exemple, la spécification XML canonique impose l'utilisation du format d'encodage de caractères UTF-8, encodage qui effectue un pont entre la norme actuelle ASCII (américaine) et les futures normes UNICODE et UCS (internationales).[60]

Suite à un tel prétraitement, les documents XML sont moins vulnérables à une simple transformation du format d'encodage, transformation transparente à l'utilisateur, mais qui invaliderait immédiatement la signature.[61] Les institutions d'archivage ne font rien d'autre quand elles migrent des formats peu utilisés vers des formats plus communs, réduisant ainsi le nombre de formats d'encodage dont elles doivent assurer la lisibilité dans le temps.

4.4 — Conclusion

Le tableau des approches techniques actuellement proposées pour permettre de conserver la signature électronique et ses fonctionnalités se décline ainsi comme suit :

(1) *La re-signature* : cette solution est fondée sur une analyse de risque centrée sur le problème de l'augmentation de la vulnérabilité des signatures cryptographiques. Elle ne s'intéresse pas au problème posé par la conservation simultanée de documents intelligibles et de signatures vérifiables ;

(2) *L'utilisation des équipements d'originaux*, soit par leur *conservation*, soit par

---

[58] W3C, *Canonical XML Version 1.0*.
[59] W3C, *Le W3C publie la recommandation XML Canonique 1.0*, communiqué de presse.
[60] Voir http://www.unicode.org.
[61] Notez que ceci est totalement indépendant du fait que le format XML soit « non-propriétaire »: le statut de « norme ouverte » ne le soustrait pas à la logique des avancées techniques et des exigences industrielles qui font évoluer les formats d'encodage, évolution à la source du problème ici considéré.

leur *émulation* : la première option n'est envisagée sérieusement par aucune institution d'archivage et ne se conçoit que dans les contextes muséaux où la valeur *intrinsèque* du document pourrait justifier la préservation des équipements d'origine[62] ; la seconde option est difficile à opérationnaliser sur grande échelle, tant sous un angle économique que sous celui de l'ingénierie logicielle, et semble devoir se confiner à des applications spécifiques[63] ;

(3) *La canonicalisation* : cette approche ne peut que surseoir temporairement au problème de l'obsolescence des formats d'encodage, sans pour autant l'éliminer.

Ces trois approches partagent un a priori fondamental : *l'authenticité du document électronique est assurée par la préservation de l'intégrité de la chaîne de bits le représentant*. Cette conception de l'authenticité électronique doit être contrastée avec celle adoptée par la profession ayant pour fonction historique d'assurer l'intégrité de la preuve documentaire, celle des archivistes.

[62] Par exemple dans le cas de la conservation des premiers enregistrements sonores sur rouleaux de cire d'Edison.
[63] Par exemple, l'émulation de jeux vidéo.

5. Réponses archivistiques à la conservation de la signature numérique

Si la signature cryptographique n'a pas connu l'essor extraordinaire qui lui semblait promis à l'époque de la rédaction de la Directive, le désir des gouvernements d'augmenter l'efficacité des administrations publiques à l'aide des technologies de l'information n'a pas lui diminué. Ainsi, des projets d'infrastructures à clés publiques visant à permettre les échanges sécurisés de données entre entités administratives sont en développement dans de nombreux pays, entre autres aux Etats-Unis, au Canada et en Australie. Les archives nationales de ces pays ont ainsi été confrontées directement au problème de la conservation de documents électroniques signés. Ces institutions ont énoncé un certain nombre de solutions à travers des documents d'orientation, particulièrement ceux des archives nationales américaines **(5.1)**, australiennes **(5.2)** et canadiennes **(5.3)**.

5.1 — Archives Nationales Américaines (NARA)

Si les Etats-Unis ont légiféré de façon à reconnaître à la signature électronique une valeur probante,[64] ils n'ont pas accordé un statut spécial à la signature cryptographique.[65] Cependant, l'Institut National des Standards et Technologies (NIST) dirige le développement d'une IGC gouvernementale fédérale, en collaboration avec la communauté technique et l'industrie. Par conséquent, les Archives Nationales Américaines (*National Archives and Records Administration*, « NARA ») ont publié en 2000 des recommandations dans le but de conseiller les diverses administrations publiques qui s'attendent à créer, conserver, et éventuellement à transférer à NARA, des documents électroniques signés.[66]

L'analyse de NARA distingue entre le *contenu*, le *contexte* et la *structure* d'un document électronique, notant que

> « pour qu'un document d'archive demeure fiable, authentique, […] il est nécessaire de préserver son contenu, contexte, et parfois, sa structure. »[67]

---

[64] « Government Paperwork Elimination Act », P.L. 105-277 ; « Electronic Signatures in Global and National Commerce Act », P.L. 106-229.
[65] Malgré les recommandations de l'American Bar Association à cet égard — voir Digital Signature Guidelines, *op. cit.*
[66] National Archives and Records Administration (2000), « Records Management Guidance for Agencies Implementing Electronic Signature Technologies », Washington, D.C., October 2000.
[67] *Ibid,* p. 7.

La préservation de la structure d'un document électronique implique que « son format physique et logique, ainsi que les relations entre les éléments qui composent le document, demeurent intacts ».[68] Ainsi, la préservation de la structure du document signé implique le respect de son intégrité physique et logique, avec la conséquence qu'il est alors nécessaire de :

> « … de conserver les équipements matériels et logiciels ayant servi à la création de la signature (c.à.d. puces et algorithmes de signature) de façon à ce que le document d'archive puisse être validé à un moment ultérieur. »[69]

Un service administratif peut cependant choisir de préserver le contenu et le contexte d'un document électronique, sans se préoccuper de préserver sa structure, structure susceptible d'être modifiée par une migration du format logique. Dans ce cas, NARA exige que soient préservées des informations contextuelles supplémentaires qui documentent, d'une part, l'existence et la validité de la signature électronique, et d'autre part, les mécanismes en place au moment de la signature du document.

NARA suggère que le choix entre la première et la seconde approche s'effectue selon les besoins du service administratif en question, les risques et les responsabilités impliquées, et la faisabilité de la solution relativement aux ressources disponibles. NARA suggère également que les services administratifs préfèrent la seconde approche dans le cas de documents d'archive soumis à une période de rétention de longue durée, en soulignant qu'elle aura pour effet de les protéger des effets de l'obsolescence technologique.

Quelle que soit l'approche choisie, NARA exige que dans le cas de documents d'archives permanents,

> « … les entités administratives doivent s'assurer que le nom du signataire électronique, en toutes lettres, de même que la date de l'exécution de la signature, soient inclus dans toute représentation lisible du document électronique — par exemple, version imprimée ou à l'écran. »[70]

Cette dernière exigence vise à assurer que, quels que soient les moyens technologiques mis en œuvre, le nom du signataire soit préservé en tant qu'élément du document d'archive et lui soit attaché de façon à en être indissociable.

---

[68] *Ibid,* p. 7.
[69] *Ibid*, p. 7.
[70] *Ibid*, p. 33.

5.2 — Archives Nationales de l'Australie

Depuis 2001, toutes les entités administratives du Gouvernement Australien doivent se conformer à *Gatekeeper*®, un ensemble réglementaire encadrant la PKI Fédérale, dans toutes les situations où un système d'authentification électronique est requis pour la fourniture d'un service gouvernemental. Par conséquent, les Archives Nationales de l'Australie ont publié en mai 2004 des recommandations relatives à l'archivage de documents signés électroniquement.[71]

Le document suggère aux services administratifs d'effectuer une analyse de risque fondée sur le besoin éventuel de démontrer la validité de la signature électronique dans un futur contentieux. Si le risque d'une telle éventualité est bas ou moyen, le document suggère le recours aux métadonnées pour consigner l'existence et la validité de la signature, en y incluant:

(1) L'identificateur unique du certificat à clé publique concerné et de l'organisation l'ayant émis ;

(2) Les informations relatives à la signature numérique associée au document — par exemple, l'algorithme utilisé ;

(3) Les informations permettant de déterminer l'heure et la date à laquelle la signature numérique a été appliquée et/ou vérifiée avec succès.

Si le risque d'un futur contentieux est élevé, les Archives recommandent aux services administratifs d'implanter un plan de gestion de clés qui procure l'accès à l'ensemble des informations nécessaires à la vérification de la signature pour la durée de vie du document d'archive. Un tel plan recouvre la conservation des certificats à clé publique relatifs à la signature, des listes de révocations, des tampons d'horodatage, et des informations relatives aux audits du système.

Dans le cas de documents qui seront éventuellement transférés aux Archives Nationales, les recommandations soulignent qu'au moment du transfert, il est peu probable qu'il demeure quelque raison pour que les signatures électroniques associées aux documents conservent leurs fonctionnalités.[72] Par conséquent,

> « Pour pouvoir préserver la qualité de ses collections, les Archives Nationales doivent

---

[71] National Archives of Australia (2004), « Recordkeeping and Online Security Process : Guidelines for Managing Commonwealth Records Created or Received Using Authentication or Encryption », http://www.naa.gov.au/recordkeeping/er/security.html.

[72] « … it is unlikely that there will be a continuing business need for any attached digital signatures to remain functional », *ibid*. p. 36.

> pouvoir s'assurer que les documents d'archive transférés sous son autorité conservent les informations contextuelles nécessaires au maintien de l'intégrité de ces documents. […] Il n'est pas possible pour les Archives Nationales de pouvoir obtenir et conserver l'ensemble des éléments des procédés d'authentification de façon à pouvoir assurer la fonctionnalité de ces procédés dans le temps. Les Archives Nationales seront dans l'incapacité de valider de nouveau les signatures numériques associées aux documents d'archive, parce qu'elles ne tenteront pas de se procurer les clés publiques concernées […] (ou tout autre mécanisme similaire). »[73]

Ce dernier constat est réitéré de façon similaire par les Archives Nationales du Canada.

5.3 — Archives Nationales du Canada

En 1999, le gouvernement canadien dévoilait un plan ambitieux prévoyant de rendre l'ensemble des programmes et services fédéraux disponible aux citoyens de façon électronique à partir de 2005. Un élément essentiel de ce plan consiste en l'établissement d'une « Infrastructure à Clé Publique du Gouvernement Canadien », infrastructure à même de répondre aux exigences de sécurité de tels services électroniques.[74]

Par conséquent, les Archives Nationales du Canada ont publié en 2001 des « lignes directrices » relatives à la préservation des documents électroniques signés.[75] Elles indiquent que les Archives Nationales n'ont pas l'intention d'accorder à la signature électronique un statut particulier en tant que moyen de preuve. En fait,

> "les Archives Nationales […] continueront de confirmer l'intégrité et l'authentification de tout document d'après son emplacement dans le système de gestion des documents d'une organisation au cours des activités habituelles de celle-ci et selon la preuve que cette organisation se fiait sur les documents de ce système."

Ainsi, du point de vue des Archives Nationales, quel que soit le rôle que la signature électronique ait pu jouer dans le cycle de vie du document préalablement à son transfert aux Archives, la signature aura, à partir de ce moment, cessé d'être utile en tant que moyen de preuve. En conséquence,

> "les Archives nationales n'essayeront pas de conserver l'habileté de revérifier la signature numérique après le transfert des documents ou de conserver les traces d'une signature numérique produite d'après le système actuel d'ICP du gouvernement du Canada. »

---

[73] *Ibid,* p. 36.
[74] Voir http:// http://www.solutions.gc.ca/pki-icp/.
[75] Bibliothèque et Archives Canada (2001), « Lignes directrices concernant les documents chiffrés et signés numériquement selon une Infrastructure à clé publique », http://www.collectionscanada.ca/06/0618_f.html.

Les Archives Nationales du Canada proposent ainsi de confiner la signature cryptographique à un rôle auxiliaire, plutôt que d'en faire le principal de moyen de preuve sous-tendant l'évaluation de l'authenticité d'un document électronique. Dans le contexte d'institutions confrontées à des budgets toujours rétrécissant, n'ayant ni les moyens, ni l'expertise pour mettre en place les infrastructures technologiques nécessaires à la préservation de documents électroniques signés, une telle approche n'est pas dénuée de logique.

5.4 — Conclusion

Du point de vue des institutions archivistiques confrontés au besoin de développer des politiques relatives à la préservation de documents électroniques signés, trois solutions s'offrent:

(1) *Préserver les signatures* et l'ensemble de la mécanique permettant de les valider. Ce choix suppose la mise en place de moyens considérables, tel que décrits à la section 4, et laisse en suspens la question de l'intelligibilité des documents ;

(2) *Enregistrer la trace des signatures sous forme de méta-données*. Cette solution n'exige que peu de moyens techniques, et conserve la trace de la signature et de sa vérification en tant qu'éléments susceptibles de renforcer l'inférence d'authenticité attribuée par l'archiviste au document ;

(3) *Éliminer les signatures.* Cette option demande le minimum d'adaptation aux institutions archivistiques, mais appauvrit la description du document, en occultant l'existence de ce mécanisme de sécurité.

Les divergences entre les solutions techniques décrites à la section 4 et les recommandations adoptées par les institutions archivistiques sont remarquables. Elles témoignent d'approches différentes au problème de la preuve documentaire électronique qui demandent à être expliquées et confrontées, de façon à en tirer les leçons qui s'imposent.

6. Conclusion et recommandations

Ce rapport fait le constat d'un écart important entre trois communautés concernées par l'analyse d'un même objet, la signature électronique fondée sur la cryptographie à clé publique. Si la communauté cryptographique a proposé qu'elle offrait l'équivalent électronique de la signature manuscrite, si la communauté juridique lui a accordé un accueil chaleureux en définissant un cadre où sous certaines conditions, elle acquiert une force probante équivalente à la signature manuscrite, la communauté archivistique est demeurée réservée.

Cette réserve s'explique quand on sait que la communauté archivistique a déjà effectué un certain nombre de constats relatifs à la préservation de documents électroniques authentiques, notamment à travers les travaux du projet InterPARES.[76] Trois de ces constats sont directement applicables à la question de la conservation des documents électroniques signés, ceux articulant (a) la distinction entre « authenticité » et « *authentication* », (b) la notion de cycle de vie du document, et (c) la relation entre intégrité physique et authenticité d'un document électronique.

6.1 — Authenticité et « authentication »

Du point de vue de la communauté archivistique, la signature électronique fournit un service d' « *authentication* »[77] et non pas une mesure d'*authenticité*. En archivistique, l'*authentication* d'un document consiste en une attestation de son authenticité à un moment spécifique.[78] Dans l'univers électronique, cette attestation est généralement effectuée après une transmission du document dans l'espace. Elle n'est équivalente ni à l'authenticité des archivistes (une qualité conférée à un document selon le mode, la forme et l'état de sa

---

[76] Le projet InterPARES vise à déterminer des principes archivistiques pertinents à la conservation de documents électroniques authentiques. Il regroupe des représentants de nombreuses archives nationales, incluant la Direction des archives de France. Voir Duranti, L. (1998). *Diplomatics : new uses for an old science*. Lanham, Md., Scarecrow Press.

[77] Il n'existe pas de traduction française satisfaisante du terme anglais « *authentication* ». En informatique, il se définit comme « le procédé matériel ou électronique visant à établir de façon formelle et intangible l'identification des parties à un échange ou une transaction électronique », de Lamberterie, *op. cit.*, p. 36.

[78] « In common usage, authentication is understood as a declaration of a record's authenticity at a specific point in time by a juridical person entrusted with the authority to make such a declaration. It takes the form of an authoritative statement (which may be in the form of words or symbols) that is added to or inserted in the record attesting that the record is authentic », MacNeil et al. (2002), « Authenticity Task Force Report », *in The Long-Term Preservation of Authentic Electronic Records : Findings of the InterPARES project,* p. 2.

transmission et préservation dans l'espace et le temps),[79] ni au concept d'authenticité du droit civil, (la force probante résultant de l'exécution de certains formalismes par un officier public).[80] Du point de vue des archivistes, la signature numérique ne constitue donc qu'un seul des éléments susceptibles de permettre d'inférer la force probante d'un écrit archivé.

6.2 — La chaîne de préservation

L' *authentication* qui résulte de la validation d'une signature numérique n'est effectuée qu'à un moment précis de la vie du document. Les archivistes infèrent l'authenticité d'un écrit en se fondant sur le principe du respect de la « chaîne de préservation », c'est-à-dire, l'ensemble des contrôles et des procédures qui assurent l'identité et l'intégrité d'un document au travers la totalité de son cycle de vie. Alors que la Directive européenne (et le droit français qui en découle) confère à la validation de la signature une valeur prépondérante, presque exclusive, au sein de cette chaîne, les archivistes ne la considèrent que comme un maillon parmi d'autres de cette chaîne. Ainsi, le projet InterPARES offre-t-il deux ensembles de critères pour évaluer l'authenticité des documents électroniques, le premier à être utilisé pour jauger la capacité d'un système d'information à produire des documents d'archives authentiques, le second pour la production de copies conformes de documents d'archives, critères fondés sur la *documentation de l'ensemble du processsus de préservation*.[81]

6.3 — Intégrité physique

Dans l'univers du document papier, l'archivistique traditionnelle peut, en partie du moins, inférer l'authenticité d'un document à partir de l'intégrité de son support physique. Dans l'univers du document électronique, où le support physique d'un document correspond à son encodage binaire enregistré sur un support magnétique ou optique, ce repère disparaît, pour deux raisons :

- D'une part, cet encodage binaire n'entretient aucune relation particulière avec son support physique, pouvant être recopié à l'infini sans souffrir de dégradation ;

- D'autre part, la chaîne de bits qui forme cet encodage[82] est susceptible d'être modifiée, au fil des migrations nécessaires pour préserver

---

[79] Voir Duranti, *ibid.*; Duranti, L., T. Eastwood, et al. (2002). *Preservation of the Integrity of Electronic Records*. Dordrecht, Kluwer Academic Publishers., p. 110

[80] Flour, J. (1972), « Sur une notion nouvelle d'authenticité (Commentaire des articles 11 et 12 du décret no. 71-041 du 26 novembre 1971) (a) », *Desfrenois* **92**: 977–1017.

[81] MacNeil, *ibid.*

[82] En anglais, *bitstring*.

l'intelligibilité du document.[83]

Or, si ces manipulations ont pour effet irrémédiable de modifier la chaîne de bits sous-tendant au document, elles n'ont pas nécessairement pour conséquence d'infirmer son authenticité : il faut plutôt pouvoir élaborer les critères permettant d'indiquer quelles manipulations sont compatibles avec la mission de l'archiviste. En contrepartie, il est absolument certain qu'un document dont on a scrupuleusement préservé l'intégrité physique, mais qui soit devenu illisible ne peut être qualifié d'authentique au sens archivistique du terme! C'est ainsi que les chercheurs d'InterPARES en arrivent à la conclusion qu'

> « il n'est pas possible de préserver un écrit électronique en tant qu'*objet physique entreposé*; il est uniquement possible de préserver les moyens de rendre ce document manifeste. »[84]

Ces trois constats soulignent que la réserve des archivistes face aux technologies de signature numérique n'est pas simplement issue d'un atavisme professionnel mal placé, mais plutôt d'une analyse cohérente des implications des technologies de l'information pour la pratique archivistique.

Alors même que de plus en plus de services administratifs et de transactions commerciales sont possibles par l'entremise de réseaux électroniques, la preuve documentaire demeure un instrument simple et durable, essentiels aux administrés et aux consommateurs pour faire valoir leurs droits et apporter la sérénité nécessaire aux échanges commerciaux.

Une preuve documentaire dont la complexité technique la met hors de portée de ses usagers et des professions chargées de l'administrer, ne remplit plus les objectifs de stabilité juridique et sociale envisagés par les rédacteurs du Code Civil. Il est donc essentiel que l'adaptation d'un outil aussi performant au contexte électronique implique l'ensemble des professions concernées par l'administration de la preuve documentaire — au premier chef, celle qui a charge de la préserver dans le temps.

---

[83] Voir Thibodeau, *op. cit.*
[84] Voir Duranti et al., (2002) *Strategy Task Force Report,* p. 4.