Projet e-Justice : rapport intermédiaire : Commission 4 : droit de la preuve

Poullet, Yves; Demoulin, Marie; Gobert, Didier; Lazaro, Christophe; Leroux, Grégory

Publication date:
2001

Document Version
le PDF de l'éditeur

PROJET e-JUSTICE

Rapport intermédiaire

Commission IV
DROIT DE LA PREUVE

Sous la direction du
Professeur Yves POULLET
Doyen de la faculté de droit

Marie DEMOULIN
Didier GOBERT
Christophe LAZARO
Olivier LEROUX

1er octobre 2001

SOMMAIRE

PRESENTATION

Dans le cadre du projet e-Justice et des travaux de la Commission IV sur le droit de la preuve dirigée par M. le doyen Y. Poullet, le présent rapport vise à fournir une analyse de trois problématiques distinctes : la certification du contenu des actes à caractère juridique ainsi que des acteurs du monde de la justice ; la conservation et la datation de documents électroniques ; et enfin l'acte authentique électronique.

En comparaison aux problèmes étudiés par ailleurs, ces deux derniers thèmes s'avèrent d'une amplitude et d'une généralité telles qu'il a été nécessaire, dans un premier temps, de cibler davantage notre recherche sur des sujets spécifiques.

Il s'est agi, pour chacune des trois questions envisagées, de les évaluer au regard de la législation existante, de souligner les problèmes qui se posent et de dégager les premières pistes de solutions concrètes, voire des propositions de dispositions législatives.

A ce stade, le rapport est conçu comme un document de travail et de réflexion destiné à ouvrir le débat entre tous les intéressés. Il représente une collection d'analyses, de pistes de réflexion et de recommandations concrètes susceptibles de nourrir des discussions, non seulement au sein de la Commission IV sur le droit de la preuve, mais également avec les autres commissions.

Les échanges, fondés sur ce rapport intermédiaire, devraient nous amener à compléter, affiner, nuancer ou reconsidérer certaines de nos analyses et propositions. Ces confrontations et réflexions nous permettront d'aboutir, au terme du troisième volet du projet e-Justice, à un rapport final proposant des solutions pratiques aux différents problèmes rencontrés.

CHAPITRE I

LA CERTIFICATION ET LA SECURISATION DES ECHANGES DE DONNEES

Table des matières

CHAPITRE I

CERTIFICATION ET SECURISATION DES ECHANGES DE DONNEES

I. INTRODUCTION

Confrontée au développement irrésistible de la société de l'information, la Justice ne peut plus aujourd'hui faire l'économie d'une réflexion approfondie quant à l'adéquation de ses modes de fonctionnements et outils traditionnels avec les nouvelles technologies de l'information et de la communication (NTIC).

Il ne fait en effet aucun doute qu'une utilisation optimale des nouvelles technologies de l'information et de la communication permettrait à la Justice de guérir l'un ou l'autre de ses maux (lenteur, arriéré judiciaire, rigidité bureaucratique…) ou, plus généralement, de tendre vers une meilleure administration. De même, un bon niveau de sécurité technique pourrait conforter, d'avantage peut-être que les modes traditionnels, la dématérialisation de certains actes à contenu juridique. Toutefois, l'adaptation de ces méthodes informatiques à des concepts et usages développés autour de l'écrit et quasi exclusivement imprégnés de la philosophie du 'papier'[1] ne se fera pas sans une profonde remise en question, tant des arcanes de la procédure que des moyens techniques.

Il n'est donc pas exagéré de prétendre que l'élaboration d'une plate-forme de justice électronique engendrera un chantier colossal, soulevant de très nombreuses questions, parmi lesquelles figure la problématique relative à la certification du contenu des actes mais aussi des différents acteurs de la Justice.

Ainsi, dans un contexte dématérialisé, où les parties ne se rencontrent peut-être jamais physiquement et où l'authentification de l'identité de chacun s'avère être l'une des clés essentielles de la confiance, comment garantir que tel acte provient bien de telle partie ? Que les actes tels qu'ils ont été communiqués entre parties ou notifiés par le greffe sont bel et bien conformes lors de l'envoi et de la réception ? Que le dossier de la procédure n'a pas été altéré ? Que la confidentialité est assurée ?

La chaîne de la justice étant ouverte à de nombreux intervenants tels que les membres de l'administration judiciaire (magistrats, greffiers, juges suppléants, juges de complément, services de police, services de médiation…), les auxiliaires de justice (avocats, notaires, huissiers de justice, autorités ordinales, experts judiciaires…) et, bien entendu les justiciables (personnes, physiques ou morales, organisations syndicales …), il convient de veiller à mettre en place un système susceptible de pallier aux difficultés inhérentes aux particularités des NTIC (anonymat, volatilité des données) afin d'offrir aux justiciables un système judiciaire présentant au moins autant de garanties que l'administration traditionnelle de la justice. En un mot, il convient de garantir la confiance des justiciables comme celle des intervenants

[1] P. MALINVAUD, *Introduction à l'étude du droit*, Paris, Litec, 8 ème éd., 1998, v. n°257. L'Ordonnance de Moulins posa dès 1566 la règle de la preuve écrite des actes juridiques.

judiciaires dans ces nouvelles technologies, trop souvent génératrices de sentiments de crainte[2].

Cette sécurisation vise à assurer la disponibilité et le contrôle de l'accès aux systèmes informatiques, l'intégrité et la confidentialité des informations échangées, l'authentification de l'émetteur et du récepteur (chaque personne est bien celle qu'elle prétend être), la non répudiation (soit la non contestation de la réception d'un message) par l'émetteur de cette information, l'archivage et l'horodatage ainsi que la conservation des données échangées, en vue de conférer aux documents électroniques une valeur juridique (en terme de preuve) égale ou même supérieure aux documents papiers correspondants. Ce n'est que moyennant la mise en place de systèmes sécurisés d'échange électronique d'information parant les documents électroniques de garanties comparables à celle du papier que de tels documents électroniques pourront un jour valoir dans le cadre d'une procédure judiciaire[3], les conditions de la force probante de l'écrit et de la signature électronique étant liées à la fiabilité des systèmes et à l'intégrité des données. Or, par nature, la sécurité est le point faible des réseaux ouverts.

Sans empiéter sur les questions propres à l'acte authentique électronique plus largement développées par ailleurs[4], la présente étude entend examiner les différentes questions relatives à la certification tant du contenu des actes communiqués par voie électronique que des acteurs de l'e-justice, condition *sine qua non* du fonctionnement du système.

Après avoir explicité les différentes implications techniques et juridiques de la certification et de la cryptographie, nous analyserons, dans un deuxième temps les conséquences pratiques et juridiques que l'adoption de ces systèmes par le monde judiciaire (au sens large) ne manqueront pas d'occasionner. Enfin, dans un troisième temps, nous formulerons, sous la forme d'une synthèse, les premières ébauches de solutions.

[2] En réalité, plus que la confiance, il s'agit de garantir la sécurité du système par l'élaboration de normes juridiques et techniques susceptibles de protéger le dossier informatisé de la procédure de toute altération. Or, le propre de la confiance n'est-il pas, justement, d'être en mesure de se priver de règles…

[3] P. VAN EECKE, "Bewijsrecht en digitale handtekeningen : nieuwe perspectieven", in *Tendensen in het Bedrijfsrecht, de elektronische handel*, Bruxelles, Bruylant, 1999, p. 216 : "Elektronische documenten moeten evenzeer kunnen beantwoorden aan een aantal vereisten waardoor het rederlijkerwijze verantwoord is om deze documenten in een gerechtelijke procedure te kunnen vertrouwen".

[4] Voy. le chapitre consacré à l'acte authentique électronique.

II. CERTIFICATION : NOTIONS ET CADRE JURIDIQUE

A. Cadre juridique de la certification

Le souhait de donner à la signature électronique et aux autorités de certification un cadre juridique clair[5] est repris dans la directive européenne 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques[6], laquelle partait du constat qu'il était urgent de disposer d'un cadre juridique harmonisé sur la question au niveau européen, afin que des initiatives éparses et divergentes n'entravent le fonctionnement du marché intérieur et ne portent atteinte à la confiance dans les nouvelles technologies et, *in fine*, à leur acceptation générale. La garantie de la confiance (et son corollaire de sécurité) était ainsi reconnue comme une nécessité absolue pour le développement des échanges des communications par voie électronique et du commerce électronique notamment[7].

Cette directive poursuit deux objectifs majeurs. D'une part, elle entend faire reconnaître par l'ensemble des pays européens la signature électronique, l'identité de l'expéditeur étant assurée par la délivrance d'un certificat émis par un prestataire de service de certification. D'autre part, elle vise à mettre en place un cadre légal pour les prestataires de service de certification. La directive entend donc appréhender de manière globale la question de la sécurisation de la communication électronique de données en prévoyant que l'utilisation de la signature électronique avancée conçue au moyen d'un dispositif sécurisé de création de signature électronique et combinée à un certificat qualifié (au sens de la directive) permet d'authentifier de manière certaine l'identité de du signataire de l'acte, ainsi que d'assurer l'intégrité du contenu de l'acte.

Cette directive a, en droit belge, fait l'objet d'une transposition en deux temps. La première loi (relative notamment à la signature électronique, cfr. *infra*) vise à réformer le Code civil afin de l'ouvrir aux nouvelles techniques de signature, la seconde (relative aux prestatires de service de certification, cfr. *infra*) vise à poser les bases de la réglementation applicable aux prestataires de service de certification dans le cadre de l'utilisation de signatures électroniques. Seule une combinaison de ces deux textes permet d'assurer adéquatement la transposition en droit belge de la directive.

B. La certification : notions et principes généraux

La certification prend place dans le cadre plus large de la question relative à la sécurisation des échanges électroniques, laquelle recouvre notamment les notions de cryptographie, utilisée à des fins de confidentialité ou de signature, sur lesquelles il est essentiel de revenir avant d'étudier les implications de la certification adaptée au monde de la Justice.

---

[5] Pour une approche détaillée des négociations internationales menées quant à l'élaboration des règles de cryptologie, voyez C. GUERRIER, "Le droit actuel de la cryptologie est-il adapté aux utilisateurs actuels de l'internet ?", http://www.lex-electronica.org

[6] Directive européenne 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, L. 13/12 à 20, 19 janvier 2000. Pour une étude détaillée de la directive, voyez M. ANTOINE, D. GOBERT, "La directive européenne sur la signature électronique : vers la sécurisation des transactions sur l'Internet ?", *J.T.D.E.*, avril 2000, n°68, pp. 73 à 78.

[7] En réalité, les organisations internationales se préoccupent depuis plusieurs années déjà de la reconnaissance du document et de la signature électronique, à l'initiative, notamment, de la CNUDCI (Commission des Nations Unies pour le droit commercial international).

1. La cryptographie à des fins de confidentialité

On entend par cryptographie (ou cryptologie[8]) l'ensemble des moyens, tant logiciels que matériels, destinés à rendre une information inintelligible puis à la restituer dans son état premier[9]. On parle également de chiffrement[10]. La cryptographie est donc la science de la transformation des messages[11], dont le principe de base consiste en la conversion d'un texte compréhensible en texte inintelligible (chiffrement de confidentialité), en vue de sa transmission à une autre personne. Sur le poste de travail du destinataire, le texte chiffré est reconverti en format intelligible (déchiffrement) pour sa lecture ou son traitement.

La cryptographie utilisée à des fins de confidentialité permet notamment la protection de la vie privée, la protection des traitements d'informations nominatives, la transmission sécurisée des données sensibles à travers les réseaux internationaux ainsi que la protection contre les divulgations à des tiers non autorisés[12].

Les systèmes cryptographiques (cryptosystèmes[13]) sont nombreux et fonctionnent avec des algorithmes mathématiques puissants[14].

Une première famille de systèmes cryptographiques utilise une seule et même clé pour verrouiller le message avant l'envoi puis le déverrouiller une fois arrivé à destination. Ce système est essentiellement efficace en réseaux fermés. On parle de cryptage par clé secrète ou clé symétrique. Cette méthode, si elle a le mérite (ou le tort ?) d'être simple, pose toutefois le problème de la communication sécurisée de la clé : sans méthode de cryptage préalable, les acteurs devront recourir à d'autres moyens pour procéder secrètement à l'échange de la clé. La même clé servant à chiffrer et à déchiffrer le message, il y a évidemment lieu de veiller à ce que la transmission de la clé de chiffrement/déchiffrement soit assurée de la façon la plus sécurisée possible. Toute transmission (volontaire ou involontaire) de la clé vers des tiers autres que le destinataire original ruine toute l'économie du système puisque la confidentialité du message n'est plus assurée.

Une deuxième famille de méthodes de cryptage[15] (crée au début des années 1980) fait appel à une formule mathématique utilisant deux clés complémentaires[16] : une clé privée et une clé publique. La clé publique du destinataire du message est utilisée par l'émetteur de celui-ci et

---

[8] Pour une étude générale de la cryptologie, de son évolution ainsi que de ses moyens techniques, voy. J. HUBIN, Y. POULLET, *La sécurité informatique, entre technique et droit*, Cahiers du CRID, Story-Scientia, n° 14, 1998.

[9] T. PIETTE-COUDOL, *Echanges électroniques, certification et sécurité*, Litec, Paris, 2000, p. 15.

[10] Selon la normalisation ISO du vocabulaire de la cryptologie, le chiffrement est défini comme 'la transformation cryptographique de données en vue de produire un texte chiffré' (ISO 8730).

[11] Pour une approche tant juridique que technique de la cryptologie, voyez *Cryptologie et signature électronique*, sous la dir. de A. BENSOUSSAN et Y. LE ROUX, Paris, Hermes, 1999.

[12] A propos de la cryptographie, voyez J. DUMORTIER, P. VAN EECKE, "Naar een juridische regeling van de digitale handtekening in België", *Computerrecht*, 1997, 4, pp. 154 et s.

[13] Un cryptosystème est un procédé mathématique pour coder ou transformer d'une façon unique un message écrit en clair en un message dit chiffré afin qu'il soit inintelligible pour ceux à qui il n'est pas destiné.

[14] Les méthodes de cryptage reposent sur l'utilisation de nombres premiers générés par des algorithmes. Pour décrypter un document sans en posséder la clé, il est donc nécessaire de disposer de puissants ordinateurs capables de parcourir l'ensemble des solutions possibles jusqu'à retenir l'algorithme recherché. La fiabilité d'un système dépend de la puissance de calcul nécessaire à mettre en oeuvre pour casser le code. Il existe actuellement sur le marché de nombreuses solutions technologiques de chiffrement, tel que Clipper/Capstone, Pretty Good Privacy (PGP), DES, Entrust, etc.

[15] Parfois dénommée RSA, des initiales des noms des trois concepteurs (RIVEST, SHAMIR et ADELMAN).

[16] On parlera alors de 'bi-clés'

permet à ce dernier de chiffrer le message. La clé privée est utilisée par le destinataire du message (qui la conserve secrètement, comme le ferait le titulaire d'un code secret bancaire, le plus généralement sur une carte à puce -*smartcard*- ou directement sur un disque dur[17]) et lui permet de déchiffrer le message. On parle de cryptage par clés asymétriques, la relation mathématique existant entre ces deux clés ne permettant pas de déduire l'une à partir de l'autre. Ce système permet le chiffrement d'un message électronique, lui retirant toute signification pour les personnes non-autorisées[18], de sorte que ce qui est chiffré par une clé ne peut être déchiffré que par l'autre.

Ces moyens cryptographiques[19] (qu'ils soient symétriques ou asymétriques) ont été essentiellement utilisés pour le chiffrement de messages (simples textes, correspondances commerciales, déclarations administratives, banques de données, œuvres couvertes par le droit d'auteur, logiciels…) afin d'en garantir la confidentialité vis-à-vis de tous.

La cryptographie asymétrique permet également de signer électroniquement des messages, afin de garantir l'identité de l'émetteur du message et l'intégrité de ce dernier. Le concept de 'signature électronique' appelle quelques précisions.

2. La cryptographie à des fins de signature électronique

Le concept de 'signature électronique' est un terme générique englobant un ensemble de mécanismes techniques (code secret, cryptographie symétrique ou asymétrique, signature biométrique, etc.) méritant d'être tenus pour des signatures dans la mesure où ils permettent, à eux seuls ou en combinaison, de réaliser certaines fonctions essentielles à cette institution juridique (identification de l'auteur de l'acte, manifestation du consentement au contenu de l'acte…)[20].

La signature électronique a été introduite dans l'ordre juridique interne belge par la loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extra-judiciaire (loi dite 'signature électronique')[21] dont l'objet est de permettre d'autres alternatives à la seule signature manuscrite et de définir les effets juridiques d'autres moyens de communication que la lettre postale (notamment le courriel ou la télécopie)[22].

Cette loi modifie les dispositions du Code civil sur la production de la preuve afin de réaliser l'équivalence de la signature électronique et de la signature manuscrite sous certaines conditions, en ajoutant à l'article 1322 du Code civil un nouvel alinéa formulé comme suit :

---

[17] P. VAN EECKE, "Bewijsrecht en digitale handtekeningen : nieuwe perspectieven", in *Tendensen in het Bedrijfsrecht, de elektronische handel*, Bruxelles, Bruylant, 1999, p. 241.

[18] Pour une explication plus détaillée des différentes méthodes de cryptage, voy. T. PIETTE-COUDOL, *Echanges électroniques, certification et sécurité*, Litec, Paris, 2000, pp. 16 et s.

[19] Pour une explication détaillée, voy. S. PARISIEN et P. TRUDEL, *L'identification et la certification dans le commerce électronique*, Québec, Ed. Y. Blais Inc., 1996, p. 99 ; J. HUBIN, *La sécurité informatique, entre technique et droit*, Cahiers du Crid, n°14, Bruxelles, E. Story-Scientia, 1998, pp. 68-112.

[20] E. DAVIO, "Certification, signature et cryptographie", in E. MONTERO (éd.), *Internet face au droit*, Cahier du CRID, n° 12, Story-scientia, 1997, pp. 80 et s.

[21] Loi du 20 oct. 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *Mon. b*., 22.12.2000, p. 42.698.

[22] Pour une analyse approfondie des fonctions de la signature électronique, voyez D. GOBERT, E. MONTERO, "La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle", *D.A./O.R.*, 2000, n°53, pp. 17-39.

> *"Peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte".*

Ce nouvel alinéa entend ouvrir le concept de signature afin que puissent être recevables en justice les actes sous seing privé signés électroniquement.

C'est à dessein (et conformément à la directive européenne) que la loi a privilégié une approche neutre sur le plan technologique afin de rendre la définition compatible aux mécanismes concurrents futurs qui viendront à voir le jour. Toutefois, force est de constater que cette neutralité technologique n'est que relative puisqu'à l'heure actuelle, sur le plan technique, seule la signature digitale (ou numérique), fondée sur la cryptographie asymétrique, répond à la définition de signature électronique avancée[23].

La signature numérique (ou digitale)[24] est un mode particulier de signature électronique caractérisée par le recours à la cryptographie asymétrique (cfr. *supra*) où la clé de chiffrement est scindée en une clé privée et une clé publique. En pareille hypothèse, la signature électronique n'est, *in fine*, qu'une donnée alphanumérique chiffrée par un algorithme cryptographique dans le but évident d'éviter toute manipulation. Pareille signature numérique peut être utilisée pour n'importe quel document électronique (message de courrier électronique, logiciel, fichier de données, transfert électronique de fonds, etc.).

Ce système de cryptographie asymétrique permet, par voie électronique, la réalisation non seulement des fonctions de la signature classique, à savoir l'identification du signataire et l'expression de sa volonté d'adhérer au message signé[25], mais aussi des fonctions nouvelles telles l'assurance de l'intégrité du contenu de l'acte ainsi que la reconnaissance du document signé en qualité de document original[26]. Dans le monde d'internet, lorsqu'elle repose sur la technologie de la cryptographie asymétrique et que le message a été chiffré, elle constitue en outre le moyen de certifier l'origine et la destination du message[27].

Pratiquement, pour signer numériquement un message électronique, on utilise une fonction mathématique dite de hachage irréversible produisant un résumé du message, chiffré à l'aide de la clé privée de l'expéditeur générant une suite de données représentant le message en question par voie d'une fonction[28]. Le résultat, qui constitue la signature numérique, est alors annexé au message adressé au destinataire, lequel peut s'assurer de l'origine du message, et de l'intégrité de son contenu, en déchiffrant la signature numérique au moyen de la clé publique de l'expéditeur, puis en comparant le résultat avec le résumé obtenu en appliquant la même

---

[23] M. ANTOINE, D. GOBERT, A. SALAUN, "Le développement du commerce électronique : les nouveaux métiers de la confiance", in E. MONTERO (éd.), Cahiers du CRID, n°16, Bruxelles, Bruylant, pp. 1-31.

[24] La définition que propose ISO est la suivante : "élément rajouté à des données, ou transformation cryptographique de données, qui permet à un destinataire des données de vérifier l'origine et l'intégrité des données et protège contre leur falsification, notamment par le destinataire".

[25] D. GOBERT, "La sécurisation des échanges par la reconnaissance de la signature électronique : condition d'existence des réseaux d'avocats", in *Multimédia, le cyberavocat*, Ed. Formation permanente CUP 1999, p. 179.

[26] Y. POULLET, M. ANTOINE, "'Vers la confiance' ou comment assurer le développement du commerce électronique", *Authenticité et Informatique*, Bruxelles, Kluwer & Bruylant, 2000 : "l'original ne se conçoit plus comme le support physique sur lequel est figé le contenu d'un document mais bien comme le résultat de la signature qui fixe logiquement cette fois le document, indépendamment du support". Disponible sur http://www.fundp.ac.be

[27] Y. POULLET, M. ANTOINE, *ibid*.

[28] T. VERBIEST, E. WERY, *Le droit de l'internet et de la société de l'information*, Bruxelles, Larcier, 2001, p. 362.

fonction mathématique au message reçu[29]. Quoique complexe à première vue, cette opération s'effectue en fait par un simple "clic de souris"[30], le système de génération et de vérification de la signature électronique étant le plus souvent directement intégré au logiciel de messagerie électronique.

Sans aucun doute, cette signature digitale répond à la définition de 'signature électronique avancée' au sens de la loi 'certification'.

Toutefois, la signature électronique ne permet de garantir l'identité de l'émetteur d'un message que pour autant que la titularité de la signature électronique utilisée soit certifiée par une tierce partie susceptible de garantir le lien existant entre l'identité affichée (ou, plus exactement, de la paire de clés) et la clé publique utilisée pour vérifier la signature. C'est à cette fin que l'on recourt aux services de certification.

3. La certification

Si le chiffrage cryptographique permet de garantir l'intégrité du message, encore faut-il que soit garantie l'identité du titulaire de la clé publique. La clé publique affichée par l'expéditeur lui appartient-elle réellement ? Comment le destinataire peut-il être sûr de l'identité de l'émetteur du message ? C'est pour satisfaire ce besoin que se joint à la relation première unissant l'émetteur au destinataire une tierce partie (dite tierce partie de confiance, *trusted third party*, *TTP*[31])[32] appelée autorité de certification ou, comme dans la loi relative aux services de certification, prestataire de services de certification (PSC[33]), chargée de délivrer le certificat électronique attestant du lien formel existant entre la clé publique et un individu[34] et permettant d'assurer la publicité et le contrôle des clés publiques[35].

Le certificat électronique est alors tout document sous format électronique attestant du lien entre les données de vérification de signature électronique et un signataire[36]. Ce certificat

---

[29] P. ASHLEY, M. VANDENWAUVER, *Practical Intranet Security, overview of the state of the art and available technologies*, Kluwer Academic Publishers, Boston, 1999, p. 15 et s.

[30] Les certificats préenregistrés dans Internet Explorer de Windows (par exemple) sont divers et se réfèrent à des autorités de certification inscrites par défaut dans Windows. Les utilisateurs peuvent toutefois décider de les accepter ou d'en adopter d'autres. Les certificats permettent d'établir des sessions sécurisées lors de la connexion à certains sites. L'apparition d'un cadenas sur l'écran, lors de la connexion, prouve que l'ordinateur distant a été identifié et qu'une liaison chiffrée a pu être mise en place.

[31] American Bar Association, *Digital signature guidelines* (draft), Chicago, 1995 ; « Utah Digital Signature Legislative Facilitation Committee, Utah Digital Signature Act », *EDI-law revue*, vol. 2, n°3.

[32] On parle souvent à leur endroit de 'notaires électroniques', erronément selon nous.

[33] Le prestataire de services de certification (PSC) est défini dans la loi 'certification' comme étant : "toute personne physique ou morale qui délivre et gère des certificats ou fournit d'autres services liés aux signatures électroniques" (art. 2, 10°).

[34] On parle alors d'une Infrastructure à Clés Publiques (ICP) ou *Public Key Infrastructure* (PKI).

[35] T. VERBIEST, E. WERY, op *cit*., p. 363.

[36] Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *Mon. b*., 29 sept. 2001, art. 2, 3° : "certificat : une attestation électronique qui lie des données afférentes à la vérification de signature à une personne physique ou morale et confirme l'identité de cette personne".

étant indispensable[37], l'utilisation de la signature électronique ne peut être envisagée sans l'intervention au départ d'autorités de certification[38].

Dans le sens commun, la 'certification' s'entend comme : "une procédure par laquelle une tierce partie donne une assurance qu'un produit, un service, un système qualité, un organisme est conforme à des exigences spécifiées"[39].

Dans un document récent, la Chambre des notaires du Québec décrivait la certification électronique comme étant : "un processus formel d'identification, partiel ou total, des parties entretenant des relations commerciales. Elle s'effectue généralement par le biais d'infrastructures technologiques et l'intervention d'une tierce partie impartiale et indépendante, soit l'autorité de certification, qui, par l'émission d'un certificat d'identification, garantit, à divers niveaux et suivant des normes préétablies, l'identité des parties transigeant à distance. Elle sert à apporter la preuve formelle et objective, émanant d'une personne indépendante et impartiale de l'identité du signataire et à le lier au contenu d'un document électronique visant à manifester son consentement à un acte juridique".

On comprend aisément que 'certification' et 'signature électronique' vont de pair, pour l'élaboration d'un système sécurisé de transmission de données. Certains considèrent d'ailleurs que l'usage combiné d'une signature électronique (avancée – cfr. *infra*) et d'un certificat (qualifié – cfr. *infra*) confère plus de garantie d'intégrité au document ainsi signé que leurs équivalents papier[40].

En vue de compléter la transposition en droit belge de la directive européenne sur un cadre communautaire pour les signatures électroniques (cfr. *supra*), le gouvernement a déposé à la Chambre le 16 décembre 1999 (soit trois jours après l'approbation de la directive) un projet de loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (projet de loi dit 'certification') qui a, au terme d'un parcours législatif à rebondissements[41], finalement conduit à l'adoption de la loi 'fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification' le 14 juin 2001[42]. Le texte final correspond au projet de loi tel qu'amendé par le Sénat[43] et

---

[37] Y. POULLET, M. ANTOINE, *op cit*., "Si la confiance en effet ne peut naître de la seule activité des interlocuteurs finaux, désespérément trop virtuels, sans doute faudra-t-il s'en remettre à l'intervention de 'tiers' indépendants dont l'activité sera précisément de créer, de manière originale, les éléments de la confiance et de la sécurité. […] Il est de l'essence même de la signature électronique d'impliquer le recours à un tiers".

[38] M. ANTOINE, D. GOBERT, "Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification", *R.G.D.C.* 1998, 4/5, p. 293.

[39] A. COURET, J. IGALENS, H. PENAN, *La certification*, Paris, PUF, 1995, Coll. Que sais-je, n°3006, p. 9.

[40] P. VAN EECKE, "Bewijsrecht en digitale handtekeningen : nieuwe perspectieven", in *Tendensen in het Bedrijfsrecht, de elektronische handel*, Bruxelles, Bruylant, 1999, p. 242. Voy. *contra*, W. FORD, M. BAUM, *Secure electronic commerce : building the infrastructure for digital signatures and encryption*, April 1997, Prentice Hall, p. 420.

[41] Le projet de loi initial a été adopté avec amendements en commission de la Chambre le 15 février 2001 puis transmis au Sénat le 16 février 2001 avant d'être évoqué par celui-ci le 5 mars. Examiné en commission des finances et des affaires économiques du Sénat, le projet a été amendé à deux reprises avant d'être adopté avec amendements en commission le 17 mai 2001. Le 18 mai 2001, le projet amendé a été transmis à la Chambre pour une seconde lecture, au terme de laquelle il fut finalement adopté en séance plénière le 14 juin 2001, sans modification.

[42] Loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *Doc. Parl*., Ch. Repr., sess. Ord. 2000-2001, séance du 14 juin 2001, n°322/008, p. 3051.

[43] Projet de loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, projet amendé par le Sénat, *Doc. Parl*., Ch. Repr., sess. Ord. 2000-2001, séance du 18 mai 2001, n°322/006, p. 2907. Par rapport au projet initialement transmis par la Chambre, le Sénat avait apporté, outre des

définit le régime juridique applicable aux opérations effectuées par les prestataires de service de certification ainsi que les règles à respecter par ces derniers et les titulaires de certificats[44].

Cette loi est plus spécifique que la loi 'signature électronique' dans la mesure où elle énumère les règles moyennant lesquelles une valeur juridique est d'office reconnue à une signature électronique[45]. A ce titre, l'article 4 s'avère être la disposition centrale de la loi, puisqu'il établit :

> *"§ 4. Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale.*
> *§ 5. Une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif :*
> *— que la signature se présente sous forme électronique, ou*
> *— qu'elle ne repose pas sur un certificat qualifié, ou*
> *— qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou*
> *— qu'elle n'est pas créée par un dispositif sécurisé de création de signature".*

Le paragraphe 4 (amendé par le Sénat) vise tout simplement, en établissant le lien entre les dispositions 'signature électronique' et les dispositions 'certification', à parfaire l'équivalence entre les signatures électroniques et les signatures manuscrites.

La loi définit l'ensemble des termes relatifs à la certification et en pose les principes généraux.

a) Prestataire de service de certification (PSC)

Aux termes de l'article 2, 10° de la loi, le PSC s'entend comme :

> *"toute personne physique ou morale qui délivre et gère des certificats ou fournit d'autres services liés aux signatures électroniques".*

Le PSC (qui peut être une entité privée ou publique) est donc l'entité chargée d'établir et, par la suite, de garantir un lien formel entre une personne et une clé publique dans le cadre d'une ICP (Infrastructure à Clés Publiques – *Public Key Infrastructure*)[46]. Il ne garantit pas la signature, mais la correspondance entre la clé publique et l'identité déclarée du détenteur de la clé.

---

corrections techniques, deux modification quant au fond du texte. La première (relative à l'article 4 du projet) réalisait l'équivalence absolue entre la signature électronique et la signature manuscrite, tant pour les procédures judiciaires qu'extra-judiciaires. La seconde concernait l'article 8, modifié de telle sorte que la personne physique représentant une personne morale et faisant usage de la signature électronique puisse toujours être identifiée.

[44]Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *Mon. b*., 29 sept. 2001.

[45] P. VAN DEN BULCK, "La signature électronique : mode d'emploi", *Journal du Juriste*, Kluwer, 2000, n°**p**

[46] De façon subsidiaire, une autorité de certification peut également accomplir des fonctions d'archivage, de création et de conservation de clés asymétriques.

Aux termes de la loi, le PSC a notamment pour mission de vérifier la complémentarité des données afférentes à la création et à la vérification de signature et de délivrer un ou plusieurs certificats à toute personne qui en fait la demande[47]. Le PSC[48] se voit donc investi du rôle de témoin spécialisé chargé de vérifier qu'une clé publique correspond bien à la personne qui s'en prévaut. La crédibilité dont il jouit ne dépend que de la confiance que lui porte le destinataire. Il va de soi que la notion d'autorité de certification ne se comprend que dans le cadre d'une architecture à clé publique.

Les PSC doivent enregistrer et archiver les informations pertinentes concernant un certificat pendant le "délai utile", c'est à dire le délai nécessaire pour pouvoir fournir une preuve de la certification en justice (point i de l'annexe II de la loi du 9 juillet 2001). Cet archivage ne couvre pas les écrits eux-mêmes revêtus d'une signature électronique : cette conservation ne concerne que le certificat correspondant à la signature liée au document électronique.

Aux termes de la loi, nul PSC ne peut être contraint de demander une autorisation préalable pour exercer ses activités. Toutefois, les PSC établis en Belgique délivrant des 'certificats qualifiés' devront communiquer à l'Administration, avant le début de leurs activités[49], leur nom, l'adresse géographique de leur établissement, les coordonnées permettant de les contacter rapidement (y compris leur adresse de courrier électronique) ainsi que la preuve qu'une assurance a été souscrite en vue de couvrir leurs obligations[50].

Par ailleurs, la loi instaure également un régime d'accréditation volontaire pour les prestataires de service de certification basée sur le résultat d'une évaluation par une entité créée par la loi (conformément à la loi du 20 juillet 1990 concernant l'accréditation des organismes de certification et de contrôle), de la conformité aux exigences des annexes I, II et III, et le cas échéant, à celles liées à d'autres services et produits délivrés par les prestataires de service de certification[51]. Cette accréditation par l'administration (art. 17-18) a pour but de garantir le respect par les PSC accrédités de règles strictes quant à l'émission de certificats au moyen de dispositifs de création sécurisés. Cette accréditation établit que le PSC dispose d'un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature satisfaisant aux exigences de l'annexe III de la loi, à savoir :

- *"1. les dispositifs sécurisés de création de signature doivent au moins garantir, par les moyens techniques et procédures appropriés, que :*
  - *a) les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée ;*
  - *b) l'on puisse avoir l'assurance suffisante que les données utilisées pour la création de la signature ne puissent être trouvées par déduction et que la signature soit protégée contre toute falsification par les moyens techniques actuellement disponibles ;*

[47] Article 8 de la loi.
[48] Différents PSC belges proposent l'émission de certificats : Belsign-Globalsign (http://www.belsign.be), Isabel (http://www.isabel.be), Belgacom (http://www.e-trust.be). Parmi les importants PSC étrangers proposant leurs services en Belgique, citons : Verisign (http://www.verisign.com) et Thawte (http://www.thawte.com).
[49] Ou dans le mois de la publication de la loi pour celles ayant déjà commencé à délivrer des certificats avant même l'adoption de la loi.
[50] Art. 4 § 2.
[51] E. WERY, "La Belgique achève le cadre légal de la signature électronique et des services de certification", http://www.droit-technologie.org, 19 juin 2001.

c) les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

- *2. Les dispositifs sécurisés de création de signature ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature".*

Ce n'est que moyennant le respect des conditions fixées à l'article 17 de la loi que le PSC pourra demander son accréditation auprès de l'administration :

> *"Art. 17. § 1er. Un prestataire de service de certification qui répond aux exigences de l'annexe II, délivrant des certificats qualifiés qui répondent aux exigences de l'annexe I et qui utilise des dispositifs de création répondant aux exigences de l'annexe III, peut demander une accréditation à l'Administration. L'accréditation prévue par la présente loi se base sur le résultat d'une évaluation, par une entité visée à l'article 2, 13°, de la conformité aux exigences des annexes I, II et III, et le cas échéant, à celles liées à d'autres services et produits délivrés par les prestataires de service de certification.*
>
> *§ 2. Le Roi précise les conditions visées au § 1er et fixe :*
> *1° la procédure de délivrance, de suspension et de retrait de l'accréditation;*
> *2° les redevances dues au « Fonds pour l'accréditation » pour la délivrance, la gestion et la surveillance de l'accréditation;*
> *3° les délais d'examen de la demande;*
> *4° les modalités du contrôle des prestataires de service de certification accrédités.*
>
> *§ 3. Le choix de recourir à un prestataire de services de certification accrédité est libre".*

Le régime d'accréditation étant libre, il est possible de voir coexister sur le marché des PSC accrédités et non accrédités.

Concernant les personnes morales, la loi impose aux PSC de tenir un registre *"contenant le nom et la qualité de la personne physique qui représente la personne morale et qui fait usage de la signature liée au certificat, de telle manière qu'à chaque utilisation de cette signature, on puisse établir l'identité de la personne physique"*[52].

Enfin, la loi contient en outre d'importantes dispositions relatives aux certificats émis par des prestataires non belges[53].

Les obligations mises à charge des AC sont donc de deux types : d'une part, les obligations ayant trait au fonctionnement du mécanisme de certification et notamment à la sécurité, et, d'autre part, celles relatives à l'objet de leur activité[54]. La fonction de PSC ne se limite pas à

[52] Art. 8 § 3, modifié suite aux travaux de la commission du Sénat.

[53] Signalons toutefois que les certificats qualifiés délivrés à l'intention du public par un PSC établi dans un état membre de l'espace économique européen est assimilé aux certificats qualifiés délivrés par un PSC établi en Belgique et que les certificats qualifiés délivrés par un PSC établi dans un pays tiers seront considérs comme équivalents aux certificats qualifiés délivrés par un PSC établi en Belgique pour autant que le régime de délivrance des certificats auxquels ils sont soumis respectent les conditions posées par la directive 99/93/CE ou aient fait l'objet d'une reconnaissance par le biais d'un accord bilatéral ou multilatéral entre la Communauté européenne et des pays tiers ou des organisations internationales.

[54] M. ANTOINE, D. GOBERT, "Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification", *R.G.D.C*. 1998, 4/5, p. 293.

la seule délivrance et gestion de certificats, mais couvre également d'autres services connexes à l'usage de signatures électroniques, tels que l'archivage ou l'horodatage.

Notons enfin que l'émission d'un certificat peut s'opérer à l'intervention de deux entités distinctes où l'une (l'autorité d'enregistrement[55]) s'assure de la collecte des données nécessaires relatives notamment à l'identité du titulaire, tandis que l'autre (l'autorité de certification), disposant de l'infrastructure technique nécessaire, émet le certificat. Le PSC n'est en effet pas tenu d'assurer seul toutes les étapes du processus de certification. Il peut, pour la collecte des informations, se référer aux renseignements détenus ou récoltés par les autorités d'enregistrement. Cela n'empêche toutefois, en termes de responsabilité, que ce soit bien le PSC qui soit tenu à l'égard des utilisateurs des certificats, des dommages consécutifs aux obligations qui lui sont imposées par ou en vertu de la loi. Dans la pratique, la collecte des informations se fera très largement par l'intermédiaire de ces autorités d'enregistrement, agissant en tant que sous-traitants du PSC.

b) Certificat

Un 'certificat' y est défini comme étant :

> *"une attestation électronique qui lie des données afférentes à la vérification de signature à une personne physique ou morale et confirme l'identité de cette personne".*

En tant que tel, la loi ne définit pas les conditions de délivrance de 'certificats', mais n'envisage que la délivrance de 'certificats qualifiés'[56] dont les conditions de reconnaissance sont définies aux annexes I et II de la loi, et aux termes desquelles, un certificat qualifié est un certificat comportant :

- *"la mention indiquant que le certificat est délivré à titre de certificat qualifié*
- *l'identification du PSC ainsi que le pays dans lequel il est établi*
- *le nom du signataire ou un pseudonyme qui est identifié comme tel*
- *la possibilité d'inclure, le cas échéant, une qualité spécifique du signataire en fonction de l'usage auquel le certificat est destiné*
- *des données afférentes à la vérification de signature qui correspondent aux données pour la création de signature sous le contrôle du signataire*
- *l'indication du début et de la fin de la période de validité du certificat*
- *le code d'identité du certificat*
- *la signature électronique avancée du PSC qui délivre le certificat*
- *les limites à l'utilisation du certificat, le cas échéant et*

[55] Prenons, à titre d'exemples d'autorités d'enregistrement, les agences bancaires pour le PSC Isabel, les chambres de commerce pour Globalsign, l'Ordre francophone des avocats de Bruxelles pour Belgacom…

[56] Le certificat qualifié est défini comme étant : "un certificat qui satisfait aux exigences visées à l'annexe I de la présente loi et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II de la présente loi" (art. 2, 4°).

- *les limites à la valeur des transactions pour lesquelles le certificat peut être utilisé, le cas échéant"*[57].

De tels 'certificats qualifiés' ne peuvent être émis que par des PSC devant :

- *"faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification ;*
- *assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat ;*
- *veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision ;*
- *vérifier, par des moyens appropriés et conformes au droit national, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré ;*
- *employer du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier, des compétences au niveau de la gestion, des connaissances spécialisées en technologie des signatures électroniques et une bonne pratique des procédures de sécurité appropriées ; ils doivent également appliquer des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues ;*
- *utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument ;*
- *prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de service de certification génère des données afférentes à la création de signature, garantir la confidentialité au cours du processus de génération de ces données ;*
- *disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la présente loi, en particulier pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée ;*
- *enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile de trente ans, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques ;*
- *ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle le prestataire de service de certification a fourni des services de gestion de clés ;*
- *avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des modalités et conditions précises d'utilisation des certificats, y compris des limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges. Cette information, qui peut être transmise par voie électronique, doit être faite par écrit et dans une langue aisément compréhensible. Des éléments pertinents de cette information doivent également être mis à la disposition, sur demande, de tiers qui se prévalent du certificat ;*
- *utiliser des systèmes fiables pour stocker les certificats sous une forme véritable, de sorte que :*
    a) seules les personnes autorisées puissent introduire et modifier des données,
    b) l'information puisse être contrôlée quant à son authenticité,
    c) les certificats ne soient disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement,

[57] Annexe I de la loi.

d) toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur"[58].

Outre l'identité, un certificat peut également permettre de vérifier éventuellement les pouvoirs et capacité du titulaire, voire même ses qualifications professionnelles (par exemple il sera possible de vérifier si la personne est bien magistrat, avocat...). Cela s'avérera bien utile dans les nombreux cas où la signature électronique attestant de l'identité de la personne ne sera pas suffisante. Ainsi, tout comme une comptabilité informatisée ne sera valablement signée électroniquement que par un expert-comptable, de nombreux échanges de messages dans le cours de l'instance ne pourront être réalisés que par certaines personnes en raison de leur qualité. La certification ne sera limitera alors pas à la seule identité, mais visera également des attributs.

c) Clés privées – clés publiques

Par 'données afférentes à la création de signature' (art. 2, 6°) et 'données afférentes à la vérification de signature' (art. 2, 8°), la loi entend :

> "*des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique avancée"*
>
> "*des données, telles que des codes ou des clés cryptographiques publiques, qui sont utilisées pour vérifier une signature électronique avancée"*

Par ces définitions quelque peu obscures à première lecture, le législateur définit en fait (sans s'y limiter tout à fait) les notions de clé privée et publique utilisés en cryptographie asymétrique[59].

[58] Annexe II de la loi.

[59] T. VERBIEST, E. WERY, *op cit.*, p. 369. Ces notions sont extensibles et, même si elles semblent en découler directement, restent ouvertes à d'autres technologies que la cryptographie asymétrique.

III. CERTIFICATION ET JUSTICE ÉLECTRONIQUE

A. Analyse des différents intervenants de la justice

Comme souligné en guise d'introduction, la chaîne de la Justice voit, sur l'ensemble de son activité, intervenir de très nombreux acteurs excédant, de loin, les seuls justiciables, conseils et magistrats.

Tous ces intervenants, dont un relevé aussi complet que possible (mais certainement non exhaustif) figure ci-après, sont susceptibles de communiquer, transmettre ou consulter des documents à contenu juridique pouvant influencer le cours de l'instance.

Il est donc essentiel, dans le cadre d'une plate-forme *e-justice*, d'être en mesure de garantir tant l'identité de ces intervenants, que la confidentialité, l'inaltérabilité du dossier de la procédure (ou, si celui-ci devait faire l'objet de modifications, l'enregistrement de ces modifications successives), l'authenticité des documents y figurant, la réception effective et l'imputabilité des messages échangés.

De manière plus fondamentale, soulignons d'emblée qu'il est également absolument nécessaire (et très certainement difficile), pour garantir la certification dans le cadre d'une ICP où l'EDI (échange de données informatiques) se définit comme l'échange de données entre des systèmes d'information conçus de manière indépendante[60], d'harmoniser les standards de messages ou de représentations de données.

Après avoir fait le relevé des différents intervenants 'judiciaires', nous analyserons leur degré d'implication ainsi que les conditions de leur certification.

1. Acteurs de l'ordre judiciaire : magistrats et greffiers

Acteurs centraux et décisifs de l'organisation judiciaire, les magistrats (du siège comme du Ministère public) se doivent de bénéficier d'un régime de certification solide.

Il s'agit en effet de garantir de manière claire que les actes juridiques émanant des magistrats (qu'il s'agisse d'arrêts, de décisions, d'ordonnances, de jugements avant-dire droit, interlocutoires ou au fond, de réquisitoires, d'avis du Parquet dans le cadre des affaires communicables…) bénéficient de systèmes de protection étendus susceptibles d'assurer leur inaltérabilité, leur inviolabilité ainsi que leur authenticité.

Notamment, il convient de veiller à ce que ces documents portent bien les signatures nécessaires et que leur contenu n'ait pas été altéré. L'article 782 du Code judiciaire dispose en effet que : *"Le jugement est signé par les juges qui l'ont prononcé, et par le greffier"*. L'article 779 du Code judiciaire pose en outre que : *"Le jugement ne peut être rendu que par le nombre prescrit de juges. Ceux-ci doivent avoir assisté à toutes les audiences de la cause. Le tout, à peine de nullité.* […]". L'original du jugement (la 'minute', qui est un acte authentique signé par le juge et le greffier), est conservé au greffe, conformément à l'article 784 du Code judiciaire qui dispose que : *"Les feuilles d'audience sont de même format et réunies, par année, en forme de registre"*.

[60] M. ANTOINE, B. VAN BASTELAER, "Le projet EDIJustice : automatisation des liens entre les différents acteurs de la procédure judiciaire", 1995, Cahiers de la CITA IJ, n°2, p. 4.

La rédaction de l'original de la décision n'est pas prescrite uniquement à des fins probatoires, mais aussi à titre de solennité. Un jugement dont les termes n'auraient pas été actés ne pourrait être invoqué car ne constituerait pas une décision de justice[61].

Un jugement rendu par voie électronique devrait donc être revêtu d'au moins deux signatures (lorsque la décision a été rendue par un juge unique), de sorte que les mêmes données devraient faire l'objet d'une double signature.

La certification de l'identité de l'émetteur devrait, à notre sens, être réalisée par l'utilisation combinée d'un certificat qualifié (au sens de l'article 2, 4° de la loi 'certification') adjoint à une signature électronique avancée au sens de la loi 'signature électronique'. Un certificat qualifié contient en effet, outre les mentions contenues dans un certificat (simple) et la signature électronique avancée du PSC, la qualité spécifique éventuelle du signataire (en l'occurrence, magistrat).

Cette qualité se doit d'être détaillée. La fonction précise doit être mentionnée afin de ne pas porter préjudice à tous les actes dans lesquels cette formalité est exigée. Ainsi, le Président d'un tribunal de première instance doit être identifié comme tel dans son certificat, pour la validité des décisions en référé, notamment. Ou un juge d'instruction dont on pourrait imaginer, pourquoi pas, qu'il communique par voie électronique un mandat d'arrêt aux services de police situés à l'autre bout du pays.

A quel PSC va-t-on confier la tâche d'émettre ces certificats ? L'administration doit-elle et peut-elle jouer un rôle ?

Pour ce qui concerne la prestation de service relative à l'émission de certificats, l'intervention de l'administration nous semble compromise pour deux raisons. Sur le plan pratique, il semblerait difficile pour l'administration de mettre en place une structure compétente susceptible de répondre aux conditions techniques imposées par la loi 'certification' pour l'établissement de certificats qualifiés, de sorte qu'il nous semble peu probable que l'administration puisse intervenir en qualité d'autorité de certification. Sur le plan juridique, la directive (considérant n°12) interdit aux Etats membres de limiter, par l'octroi de régimes d'accréditation, la concurrence dans le secteur des services de certification, de sorte que les services de certification doivent demeurer soumis au régime de libre concurrence. Une dévolution exclusive du rôle de tiers certificateur à un service de l'administration pour tous les services relevant de son organisation nous semble contraire à ce principe de libre concurrence.

Toutefois, pour ce qui concerne l'enregistrement (c'est à dire la tâche consistant à collecter l'information : *in casu*, attester de la qualité de magistrat ou de greffier en chef), en vue de garantir l'indépendance (au moins fonctionnelle) de la justice, celui-ci devrait être réalisé à l'intermédiaire d'une instance publique organiquement rattachée à la Justice. Dans cet esprit, et vu le caractère relativement administratif de la tâche, il nous apparaîtrait logique de confier cette tâche à l'un des services de la Direction Générale du Ministère de la Justice (organiquement rattaché au service du personnel de la magistrature), plutôt qu'à la Cour de cassation ou aux Cours d'appel.

[61] A. FETTWEIS, *Manuel de procédure civile*, Faculté de droit de Liège, 1987, p. 253.

L'établissement d'un tel service devrait, idéalement, se faire en concertation avec les responsables du programme FedPKI (voyez *infra*) afin de garantir l'interopérabilité des systèmes, telle que souhaitée dans la directive[62].

Concernant la certification sur le plan technique, celle-ci devrait être réalisée par des PSC accrédités. Or, comme déjà souligné *supra*, la première attente à l'égard d'un PSC est bien entendu son impartialité et son indépendance, génératrices de confiance[63]. Il conviendra donc de recourir aux services d'un PSC établi et de compétence notoire, de façon à dissiper tout doute quant à la validité des certificats émis. A ce propos, il est encore à souligner que l'article 4 § 3 de la loi 'certification' prévoit, concernant le secteur public, que : *"le Roi peut, par arrêté délibéré en Conseil des ministres, soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée. Ces exigences ne peuvent pas constituer un obstacle aux services transfrontaliers pour les citoyens"*.

Rien n'empêcherait donc le pouvoir exécutif d'adopter un arrêté royal disposant de conditions techniques particulières pour la certification des magistrats, laquelle concerne, au premier chef, l'ensemble des magistrats membres des Cours et tribunaux de l'organisation judiciaire (juges de paix et de police, juges au tribunal de première instance, du travail et de commerce, juges au tribunal d'arrondissement, juges suppléants, juges consulaires, membres des Cours d'appel et du travail, conseillers suppléants et enfin, membres de la Cour de cassation), mais également les magistrats du Ministère public auxquels il convient encore d'ajouter les juges sociaux près les tribunaux du travail[64].

Pour tout mandat à échéance fixe, il va de soi que les certificats liés à l'exercice de la fonction devraient voir leur durée de validité fixée en concordance avec le terme du mandat (ainsi en est-il des juges sociaux, dont le mandat est fixé à 5 ans, la certification de chacun d'entre eux devra indiquer, outre leur identité, leur fonction ainsi que la juridiction à laquelle ils sont rattachés).

De façon plus périphérique, il conviendra, à terme, de veiller également à la certification des services de police et de médiation[65]. La certification (pour ce qui concerne l'enregistrement) des services de la police fédérale devrait, à notre sens, dépendre d'une entité relevant du ministère de l'intérieur, afin d'éviter toute mixtion imprudente des pouvoirs. Encore une fois, cet enregistrement devrait, idéalement, être réalisée de manière coordonnée au niveau fédéral (*cfr.* FedPKI).

Les services de médiation devraient, quant à eux, faire l'objet d'une certification à l'intermédiaire du ministère de la justice, dont ils dépendent organiquement puisque placés sous l'autorité des procureurs généraux ou des magistrats désignés à cet effet[66].

---

[62] Le considérant n°5 de la directive prévoit en effet : "Il convient de promouvoir l'interopérabilité des produits de signature électronique ; conformément à l'article 14 du traité, le marché intérieur comporte un espace dans lequel la libre circulation des marchandises est assurée […]".

[63] *Trusthealth Report, Introducing to the legal acceptance of digital documents and signatures and liability of trusted third parties*, Trustworthy Health Telematics, 1996, p. 21.

[64] Bien que ceux-ci ne soient pas en tant que tel magistrats, il convient néanmoins de veiller à leur certification, dès lors qu'ils sont amenés à signer les jugements rendus par le tribunal auprès duquel ils siègent en qualité de juges sociaux, et ce, conformément aux articles 8 et s. du Code judiciaire.

[65] Articles 272*bis* et 272*ter* du Code judiciaire.

[66] Articles 176*bis* à 176*quater* du Code judiciaire.

Les services des greffes (des justices de paix, tribunaux de police, tribunaux de première instance, du travail et de commerce, des Cours d'appel et du travail et de la Cour de cassation[67]) devront également disposer de certificats propres, indépendants de celui des magistrats, et rattachés au responsable du greffe (greffier en chef)[68], par analogie au régime relatif à l'attribution de certificats aux personnes morales. Ces derniers pourraient également disposer de certificats émis par le service de certification du ministère de la justice envisagé *supra*.

La certification des greffes s'avère toute aussi essentielle que celle des magistrats eux-mêmes, le greffe servant le plus généralement d'interface entre le juge et les parties.

L'objectif est bien entendu de garantir tant l'intégrité du message envoyé et l'identité de l'émetteur que la possibilité, en cas d'altération du contenu du dossier de la procédure (modification de données, ajout ou suppression de données), d'enregistrer les modifications apportées ainsi que la version originellement envoyée. Cela ne pourra se faire que via la mise en place d'un système technique d'archivage et d'horodatage élaboré (établi et dépendant du greffe), susceptible de conserver en mémoire les différentes versions du dossier de la procédure. La force probante de l'écrit électronique est en effet subordonné à la condition qu'il soit conservé dans des conditions de nature à en garantir l'intégrité, de sorte que la question de la conservation est indissociable de la question de la preuve[69].

Concernant le cas particulier du registre de commerce, celui-ci devra être en mesure de communiquer par voie électronique tout document pour lesquels la loi lui attribue compétence. Ainsi, notamment, la preuve de l'immatriculation d'un commerçant devrait pouvoir être communiquée par voie électronique puisque toute personne physique ou morale désirant exercer une activité commerciale doit, préalablement à tout exercice, demander son immatriculation au registre de commerce du ressort du tribunal du commerce territorialement compétent[70]. Par ailleurs, tout commerçant désirant exercer une activité commerciale différente de celle déjà exercée doit demander une inscription modificative[71], ou, en cas d'arrêt de l'activité, requérir la radiation de son immatriculation[72]. Les renseignements ainsi compilés au sein du registre du commerce peuvent être consultés par différents intervenants : huissiers (pour vérifier l'identité des personnes à citer), avocats… Il faudrait dès lors prévoir une possibilité d'accès et de lecture des fichiers concernés par les destinataires habilités, moyennant identification de ces derniers par le biais de l'utilisation croisée d'un certificat qualifié et d'une signature électronique avancée.

En sus des juridictions ordinaires, il y a lieu également d'envisager la certification des juridictions extraordinaires que sont le Conseil d'Etat[73] et la Cour d'arbitrage devant laquelle des questions préjudicielles sont régulièrement portées en cours d'instance.

---

[67] Bien que l'hypothèse d'une informatisation de la justice au niveau de la Cour d'assises nous paraisse pour le moins hypothétique, signalons qu'il y aurait lieu d'attribuer au greffier du Tribunal de première instance désigné en charge du greffe de la Cour d'assises, conformément à l'article 166 du Code judiciaire, un certificat particulier, propre à la cause, dont la validité expirerait lors de la clôture de la session d'assises.

[68] Articles 157 à 176 du Code judiciaire.

[69] V. SEDALLIAN, "Preuve et signature électronique", http://www.juriscom.net, 9 mai 2000.

[70] Voyez, pour plus de précisions, l'article 4 des lois coordonnées relatives au registre de commerce.

[71] Art. 13 des lois coordonnées relatives au registre de commerce.

[72] Art. 18 des lois coordonnées relatives au registre de commerce.

[73] Concernant le Conseil d'Etat, la difficulté de situer cet organe dans la séparation traditionnelle des pouvoirs rend délicate la détermination de l'autorité compétente pour son enregistrement. "Une chose est certaine, le

2. Juridictions extra-judiciaires

Il existe en dehors de la sphère du pouvoir judiciaire différentes instances dont l'activité prend place dans le cadre de l'activité juridique au sens large, de sorte que la réflexion à leur endroit en ce qui concerne la certification ne pourrait être esquivée. Nous pensons notamment aux juridictions administratives que sont l'Office des Etrangers, le Commissariat Général aux Réfugiés et Apatrides, les Commissions permanentes de recours ainsi que les Commissions de régularisation.

3. Auxiliaires de Justice

a) Avocats

Parmi les différents auxiliaires de justice[74], les avocats occupent, à n'en pas douter, une place toute particulière dans l'administration de la justice, en tant qu'intermédiaire naturel entre les parties et le juge (via le greffe), de sorte que la question de leur certification apparaît comme centrale, et ce, de manière plus pressante encore depuis la récente modification du Code judiciaire permettant de réaliser le dépôt de conclusions au greffe par voie électronique[75].

Selon nous, il appartient aux Ordres de réglementer l'emploi des méthodes de cryptographie et de signature électronique par leurs membres.

Conscient de la nécessité de pourvoir ses membres d'une signature électronique conforme aux nouvelles exigences légales (mais également des difficultés pratiques et technique que cela soulève dans une profession pour partie encore fortement imprégnée de la culture de l'écrit 'papier'), l'Ordre français des avocats du barreau de Bruxelles a signé une convention avec l'opérateur Belgacom visant à mettre en place une police de certification développée conjointement[76].

Cette convention a pour but de doter les avocats qui le désirent de certificats authentifiant l'identité du signataire de l'acte électronique ainsi que l'intégrité du contenu de l'acte. De plus, elle permet aux avocats qui le désirent (et qui acceptent de suivre la formation adéquate) de devenir eux-mêmes autorités d'enregistrement de leurs clients par l'émission de certificats "tiers-client", de sorte qu'ils peuvent, dès l'entame des relations, proposer un certificat à leurs clients désireux d'entretenir une relation virtuelle, leur offrant ainsi toutes les garanties d'authentification, de confidentialité et de maintien de l'intégrité.

Conseil d'Etat ne fait pas partie du pouvoir judiciaire" avait écrit P. LEWALLE (*Contentieux administratif*, Faculté de droit de Liège, 1997, p. 289). La localisation de l'article 107*quinquies* de la Constitution lui donnant sa base constitutionnelle se situant en-dehors des dispositions relatives au pouvoir judiciaire semblent en effet indiquer qu'il n'en fasse pas partie. La majeure partie de la doctrine, perplexe, tend à considérer le Conseil d'Etat comme indépendant ou relevant du 'pouvoir juridictionnel' (DELPEREE F., DEPRE S., *Le système constitutionnel*, Bruxelles, Larcier, 1998, pp. 237-238).

[74] Certains auteurs contestent que cette expression puisse être applicable aux avocats, à propos desquels ils considèrent plus appropriés l'emploi de l'expression 'organe de justice'. E. REUMONT, *Permanence et devoirs de la profession d'avocat*, Bruxelles, Bruylant, 1947, p. 42-43 ; C. LECLERCQ, *Devoirs et prérogatives de l'avocat*, Bruxelles, Bruylant, 1999, p. 25.

[75] Les actes de procédure nécessitant la signature de l'avocat sont nombreux : conclusions, requêtes, pourvoi…

[76] F. DECHAMPS, "L'Ordre français des avocats bruxellois se met à la signature électronique", disponible sur http://www.droit-technologie.org

Aux termes de cet accord, l'Ordre est l'autorité d'enregistrement et assure le relais des modifications et retraits des certificats puisqu'ils indiqueront des données gérées par l'Ordre telles que la qualité d'avocat, l'appartenance à une association ou à un groupement d'avocats, les activités préférentielles, les spécialités reconnues et les mentions honorifiques déontologiquement communicables (par exemple la qualité de membre du conseil de l'Ordre).

Outre les services de l'Ordre, des avocats seront mandatés par l'Ordre pour l'enregistrement.

Cet accord vise, à terme, à assurer une sécurité dans la relation unissant l'avocat à ses clients ou des tiers (greffes, administrations publiques…).

Cette initiative du barreau de Bruxelles est à saluer[77] et il est à espérer que d'autres barreaux ne manqueront pas de suivre les chemins ainsi tracés pour, à leur tour, proposer à leurs membres l'un ou l'autre service de certification.

Toutefois, l'attribution des rôles de certification telle qu'envisagée dans cet accord appelle quelques développements.

S'il est clair qu'une autorité ordinale (telle l'Ordre français des avocats du barreau de Bruxelles) a, dans le cadre de la certification de ses membres, un double rôle à jouer, à la fois sur les plans déontologiques et pratiques (où le barreau se doit de prendre position quant à l'emploi des systèmes de signature électronique et de cryptage[78]), il convient, en tout état de cause, de veiller à respecter les prescrits légaux en matière de certification, et notamment, les dispositions relatives au contrôle de la véracité des données.

Dans le cadre de l'accord, c'est aux autorités de l'Ordre qu'il appartient de communiquer tous les renseignements utiles concernant l'avocat en vue de leur certification par l'opérateur[79]. Ainsi, c'est notamment les services de l'Ordre qui seront chargés d'attester de la qualité d'avocat des membres pour lesquels ils demanderont la certification. Or, l'article 5 de la loi prévoit que le PSC qui délivre des certificats à l'intention du public ne peut recueillir des données personnelles que directement auprès de la personne concernée ou avec le consentement explicite de celle-ci et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat. Il s'en déduit que la délégation à l'Ordre de fournir au PSC des renseignements personnels ne peut être qu'exprès et ne pourrait porter atteinte aux dispositions de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Par ailleurs, si, en tant que tel, cette intervention ordinale (somme toute logique) ne suscite pas d'opposition particulière, la question devient plus ardue lorsqu'il s'agit d'envisager la révocation d'un certificat. Qu'adviendra-t-il en effet du certificat attestant de l'identité et de la qualité d'un avocat après que ce dernier ait fait l'objet d'une radiation de l'Ordre ? Ou d'une simple suspension ? L'Ordre peut-il exiger la révocation de ce certificat ? De même, qui au

[77] A notre connaissance, cette convention n'aurait, à l'heure de la rédaction de ces lignes, donné lieu qu'à l'émission de quelques certificats.

[78] Comme le souligne D. FESLER, il serait judicieux de recommander aux avocats qui font usage de la messagerie électronique qu'ils signent toutes communications électroniques ou semi-électroniques qu'ils destinent à des personnes extérieures à leur cabinet de sorte qu'ils soient toujours en mesure de démontrer le contenu de telles communications et que seules celles-ci puissent effectivement leur être opposées, in D. FESLER, "La signature électronique et les avocats : *quo vadimus* ? Enjeux et opportunités pour le barreau", non publié.

[79] F. DECHAMPS, *op cit*.

sein de l'Ordre sera compétent pour demander la révocation du certificat et attester de la radiation ou de la suspension ?

Aux termes de l'article 12 de la loi 'certification', la révocation d'un certificat ne peut intervenir que dans une série limitative d'hypothèses : soit à la demande du titulaire (préalablement identifié), soit *"lorsqu'il existe des raisons sérieuses pour admettre que le certificat a été délivré sur base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus conformes à la réalité ou que la confidentialité des données afférentes à la création de signature a été violée"*. La loi ne précise pas, concernant cette deuxième hypothèse, si le PSC doit agir d'initiative ou au contraire sur demande. Et dans ce dernier cas, ne précise pas à qui appartiendrait alors le droit d'initiative.

Une interprétation pratique de la loi conduit à conseiller aux PSC sous-traitant la tâche d'enregistrement à des tiers d'introduire dans leurs conventions des clauses contractuelles faisant peser sur l'autorité d'enregistrement l'obligation d'informer le PSC de toutes modifications contenues dans le certificat dont il aurait connaissance. En l'espèce, Belgacom devrait donc (si ce n'est pas le cas, ce que nous ignorons) imposer à l'Ordre de le prévenir en cas de radiation afin de lui permettre de respecter son obligation de révocation.

L'Ordre, agissant en qualité de PSC, nous semble la seule entité capable d'attester de la qualité d'avocat de ses membres. Il nous paraît donc évident que c'est bien à l'Ordre auprès duquel l'avocat est inscrit que doit incomber la charge de l'enregistrement. Toutefois, cette position justifie-t-elle l'octroi à l'autorité ordinale de décider de la révocation pure et simple d'un certificat ?

Il nous apparaît que la révocation d'un certificat est lourde de conséquence pour le titulaire qui s'en trouve privé[80]. Aussi, circonscrire au maximum le dommage susceptible d'être occasionné par la révocation d'un certificat et préserver à l'autorité ordinale le pouvoir d'attester de la qualité d'avocat, il nous semble sage de privilégier l'élaboration de certificats strictement personnels[81] à usage exclusivement professionnels dans le cadre de l'activité d'avocat, distincts d'éventuels autres certificats (à usage privé ou professionnels, mais en-dehors de l'activité d'avocat), tout comme un avocat disposera le plus généralement de deux comptes en banque (l'un privé, l'autre professionnel) auxquels seront attachées deux cartes de banque distinctes. L'article 8 de la loi '*certification*' prévoit la possibilité pour le PSC d'émettre un ou plusieurs certificats.

Par ailleurs, comme le souligne le représentant d'un PSC belge, il convient de rappeler que la révocation d'un certificat relèvera uniquement de l'effet d'annonce, puisqu'elle n'entraînera aucun retrait physique des moyens de signature et se traduira uniquement par la seule publication sur un site web déterminé (celui de l'autorité de certification, celui des autorités ordinales, celui du ministère de la justice…) d'une liste des certificats révoqués. Le destinataire d'un courrier électronique ne trouvera dans celui-ci aucune information, ni même aucun indice de l'usage abusif de la signature qui accompagne le message et du certificat qui y correspond. Le détenteur du certificat révoqué conserve donc ledit certificat et peut continuer à l'utiliser dès lors qu'il détient sa clé privée à titre exclusif, laquelle se trouve soit sur son ordinateur, soit sur une carte à puce (avec lecteur annexe) soit encore sur un *token*. Or, l'usage

[80] La révocation d'un certificat est irréversible, de sorte qu'un certificat révoqué ne peut être réactivé. Le titulaire de certificat privé de son certificat à la suite d'une révocation doit en pareille hypothèse solliciter auprès de son PSC la génération de nouvelles clés.

[81] Même si l'on pourrait imaginer l'émission de certificats pour associations d'avocats, mais ces certificats

du certificat n'est pas susceptible d'être "gelé" de l'extérieur par un tiers et, du reste, aucune technologie ne permet de l'envisager.

On soulignera à ce propos que la première version du projet de loi relative aux prestataires de service de certification imposait *expressis verbis* au destinataire d'un document signé de vérifier la validité du document signé (existence, non révocation) auprès du PSC. Cette obligation à charge du destinataire, tirée de l'article 6 de la directive[82], n'a pas été retenue dans la loi. Seul demeure dans la loi l'article 14 relatif à la responsabilité des PSC émettant des certificats qualifiés, aux termes duquel :

> *"Un prestataire de service de certification qui délivre à l'intention du public un certificat présenté comme qualifié ou qui garantit au public un tel certificat est responsable du préjudice causé à tout organisme ou personne physique ou morale qui, en bon père de famille, se fie raisonnablement à ce certificat pour ce qui est de :*
> *a) l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié;*
> *b) l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat;*
> *c) l'assurance que les données afférentes à la création de signature et celles afférentes à la vérification de signature puissent être utilisées de façon complémentaire, dans le cas où le prestataire de service de certification génère ces deux types de données;*
> *sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence […]".*

C'est par la référence *in abstracto* au 'bon père de famille' que se définit aujourd'hui l'obligation pour le destinataire de vérifier la validité du certificat auprès du PSC. A défaut de ce faire, le destinataire ne pourra pas invoquer la responsabilité du PSC en cas de dommage causé par l'usage d'un certificat pour ce qui est des données reprises à l'article 14.

Ce travail de contrôle est fastidieux. Aussi, afin de conférer à la révocation des effets plus directement décisifs et directs, et dans l'attente de solutions techniques permettant la vérification par contrôle automatique de la validité des certificats sans passer par des sites tiers, convient-il de souligner l'existence de systèmes physiques de signature électronique (tels que cartes à puces ou *token*) dont on pourrait envisager le retrait matériel. Le titulaire

[82] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, article 6 :
1. Les États membres veillent au moins à ce qu'un prestataire de service de certification qui délivre à l'intention du public un certificat présenté comme qualifié ou qui garantit au public un tel certificat soit responsable du préjudice causé à toute entité ou personne physique ou morale qui se fie raisonnablement à ce certificat pour ce qui est de:
a) l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié;
b) l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat;
c) l'assurance que les données afférentes à la création de signature et celles afférentes à la vérification de signature puissent être utilisées de façon complémentaire, dans le cas où le prestataire de service de certification génère ces deux types de données,
sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.[…]

d'un certificat privé de son outil de signature ne serait alors plus en mesure de signer numériquement aucun document.

Concernant les avocats, l'opportunité d'une telle mesure resterait toutefois à discuter. Soulignons toutefois, concernant le barreau des avocats francophones du barreau de Bruxelles, la possibilité dont dispose le bâtonnier sur base de l'article 464 du Code judiciaire de prendre toute mesure conservatoire que la prudence exige à l'égard d'un avocat à l'encontre duquel de simples 'faits reprochés' risqueraient de faire craindre que l'exercice ultérieur de son activité soit de nature à causer préjudice à des tiers ou à l'honneur de l'Ordre. Ces mesures conservatoires pouvant aller jusqu'à interdire à l'avocat concerné de fréquenter le palais pendant une période pouvant aller jusqu'à trois mois (délai susceptible d'être prolongé), on peut imaginer qu'elles englobent également le retrait du mécanisme de signature électronique.

Qu'en est-il enfin de l'épineux problème du droit éventuel des autorités ordinales à se faire remettre par un avocat sa clé privée ?

Encore une fois, conformément à la directive européenne du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, les clés privées utilisées par les avocats demeureront sous le contrôle exclusif de leurs titulaires, sans qu'il soit possible pour un Ordre quelconque d'en réclamer la remise. Les avocats ne pourraient donc, à notre sens, être tenu à la restitution de leur clé privée au bénéfice des autorités ordinales, d'autant qu'ils restent soumis au respect du secret professionnel : "l'avocat est rigoureusement tenu de garder secret ce qui lui a été confié : il ne peut trahir ce secret"[83], auquel "se rattache celui du secret de la correspondance"[84].

Toutefois, il convient de rappeler que, si signature électronique et chiffrement des messages sont, dans la pratique, souvent liés, il est possible d'imaginer que signature et chiffrement soient réalisés par deux paires de clés distinctes : l'une pour la signature, l'autre pour le chiffrement. En ce cas, cette deuxième paire de clés ne tombe pas sous le coup des dispositions de la directive et de la loi. En effet, tant la directive que la loi ne traitent que de la signature : les clés auxquelles il est fait référence ne permettent que de signer l'acte. Les clés de chiffrement ne sont donc pas couvertes par le droit exclusif du titulaire. Les autorités ordinales pourraient dès lors réclamer la clé privée de chiffrement d'un avocat (et uniquement celle-là) afin de contrôler le contenu d'un acte.

Cette question prend un tour différent si la demande de remise de clé privée (de signature et de chiffrement) intervient dans le cadre d'une perquisition ordonnée par un juge d'instruction. En pareille hypothèse, les dispositions disciplinaires relatives à la perquisition et aux saisies dans les cabinets d'avocats devront être respectées[85]. Le bâtonnier peut-il connaître de la clé privée de signature ? Doit-il la connaître ? Il appartiendra aux autorités ordinales de trancher cette délicate question au regard de leurs dispositions disciplinaires mais il nous apparaît important, à ce propos de rappeler que les titulaires de clés privées en disposent de manière exclusive.

---

[83] P. LAMBERT, Règles et usages de la profession d'avocat du barreau de Bruxelles, Bruylant, 1994, p. 439.
[84] P. LAMBERT, Règles et usages de la profession d'avocat du barreau de Bruxelles, Bruylant, 1994, p. 445.
[85] Voy. not. pour le barreau francophone de Bruxelles : M. WAGEMANS, *Recueil des règles professionnelles*, Barreau de Bruxelles, Bruxelles, 1999, n°245 et s. (*L.B.*, mai 1985, p. 270 ; *L.B.*, septembre 1980, p. 16 ; *L.B.*, Juin-juillet-août 1997, p. 366, *L.B.* février-mars 1997, p. 207 ; *L.B.*, janvier 1985, p. 160).

Cette intervention ordinale n'ira pas sans poser certaines questions de responsabilité. Ainsi, qu'en sera-t-il en cas de perte ou de vol du dispositif de création de signature électronique ? Aux termes de l'article 19 § 2 de la loi 'certification', il faut que l'avocat lui-même puisse ordonner au PSC la révocation du certificat. Or, qu'en sera-t-il dans le cadre de l'accord passé entre l'Ordre de Bruxelles et Belgacom ?

Concernant les avocats à la Cour de cassation, signalons encore que, compte tenu du fait que le Code judiciaire exige en son article 1080 qu'une requête en cassation soit *"signée tant sur la copie que sur l'original par un avocat à la Cour de cassation […] : le tout à peine de nullité"*, il est nécessaire que ces derniers bénéficient d'un service de certification attestant, outre de leur qualité d'avocat, du fait qu'ils sont bel et bien inscrits au barreau de cassation.

Enfin, pour ce qui concerne la simple suspension d'un avocat du tableau (laquelle n'a pas pour effet de faire perdre la qualité d'avocat mais simplement le retrait temporaire des prérogatives liées à l'exercice de la fonction), il nous semble qu'elle ne devrait pas entraîner de révocation du certificat (tout comme un avocat suspendu ne se voit pas priver par l'Ordre de son papier à lettre), mais une simple injonction disciplinaire faisant interdiction de faire usage du certificat pendant la durée de la suspension. A cet égard, notons que l'accord passé entre le barreau francophone de Bruxelles et Belgacom prévoit, alors que ni la directive ni la loi nationale ne l'évoquent[86], la possibilité de procéder à la suspension du certificat. Encore une fois, pareille suspension ne pourrait valoir qu'à titre d'effet d'annonce par voie d'affichage (au sens large). Cette possibilité de suspension nous paraît plus conforme qu'une véritable révocation (laquelle, rappelons-le, est irrévocable) en cas de suspension du tableau même si, *de facto*, la différence de traitement ne sera pas notable.

En tout état de cause, il nous apparaît que le certificat des avocats doit être un certificat qualifié, conforme aux dispositions de l'annexe I de la loi et fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II de la loi, seul garant des exigences d'identification[87] du signataire et permettant d'inclure, dans le certificat, la qualité du signataire.

b) Huissiers de justice

Acteurs essentiels de l'introduction et de l'exécution des décisions de justice, les huissiers de justice devront eux aussi bénéficier d'un système de certification adéquat. Ainsi, leur signature est-elle notamment exigée dans l'exploit de signification (art. 43*initio* et 862 §1, 2° C. jud.) tant en original que sur la copie. Cette exigence de signature a été considérée par la Cour de cassation comme une 'condition de validité' dont l'absence justifie une annulation sur pied de l'article 862 du Code judiciaire[88].

[86] Concernant la suspension des certificats, la directive comme la loi ne prévoient rien. Selon les dires du ministre, questionné à ce sujet en commission, c'est à dessein que cette possibilité a été exclue (alors qu'elle existe en France) afin de ne pas porter atteinte à la sécurité juridique en allégeant la responsabilité des PSC et notamment leur obligation de révoquer immédiatement à la première demande un certificat. Soucieux de garantir la confiance, le ministre estime que la suspension n'aurait pour effet que d'alléger la responsabilité des PSC au regard de leur obligation de révocation.

[87] Un certificat qualifié est, aux termes de l'article 2, 4° de la loi 'certification', un certificat satisfaisant aux exigences visées à l'annexe I de la loi et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II de la loi. Il indique, outre les mentions reprise dans le simple certificat, la signature électronique avancée du PSC, les éventuelles limites à l'utilisation du certificat ainsi qu'éventuellement une qualité spécifique du signataire, "en fonction de l'usage auquel le certificat est destiné".

[88] Cass., 18 novembre 1982, *Pas*., I, 337.

Les huissiers de justice (dont les conditions de titre, nomination, serment et résidence sont contenues aux articles 509 et suivants du Code judiciaire) devront donc eux aussi bénéficier de signatures électroniques avancées ainsi que de certificats qualifiés. Quant à l'autorité compétente pour procéder à l'enregistrement, la Chambre nationale des Huissiers de justice[89] nous paraît l'autorité compétente pour établir et garantir la qualité d'huissier de ses membres. Pour ce qui est de la certification au plan technique, nous renvoyons à ce qui a déjà été dit concernant les avocats.

Il est à noter que rien n'empêche les huissiers de justice (en tant que personnes physiques) de jouer eux-mêmes le rôle de tiers enregistreur, l'Huissier de justice en sa qualité d'officier ministériel assermenté devant pouvoir prendre une place dans le processus de certification.

c) Experts judiciaires

Le Code judiciaire contient, en ses articles 962 et suivants, les dispositions relatives à l'expertise. Lorsqu'il a été décidé, au cours d'une instance, de recourir à l'expertise (à titre principal ou à des fins d'instruction), celle-ci donnera lieu à l'établissement par l'expert d'un rapport destiné à éclairer le(s) juge(s) sur l'une ou l'autre question d'ordre essentiellement technique qui lui aurait été posée par voie de requête. Le rapport d'expertise comporte deux parties : les préliminaires et la conclusion. En vertu de l'article 979 al. 3 du Code judiciaire (modifié par la loi du 27 mai 1974), le rapport est signé par tous les experts, la signature des experts étant précédée du serment. Même si cet article ne prévoit pas la nullité du rapport en cas d'absence de signature ou de serment, de sorte qu'un tel rapport pourrait être régularisé soit par le dépôt d'un nouveau rapport dûment signé, soit par la signature du rapport par l'expert au greffe ou à l'audience[90], le rapport doit revêtir la signature de l'expert qui l'a rédigé.

Pour les mêmes raisons que celles développées *supra* concernant les avocats, il convient dès lors de veiller à ce que les rapports d'expertise délivrés dans le cadre de l'e-Justice soient pourvus de signature électronique avancée garanties par des certificats qualifiés. Ces certificats reprendront l'identité complète de l'expert. Le titre d'expert judiciaire près les tribunaux n'existant pas légalement, il n'y a pas lieu de mentionner cette qualité dans le certificat mais cela pourrait être utile en vue de déterminer la spécialité de l'expert.

d) Organisations syndicales

Conformément à l'article 728 § 3 du Code judiciaire, les travailleurs peuvent se faire représenter devant les tribunaux du travail par les délégués d'organisations représentatives d'ouvriers ou d'employés porteurs de procurations écrites pour la défense de leurs intérêts.

Les délégués d'organisations syndicales interviennent alors en qualité de conseil de leurs affiliés sur bas d'un mandat *ad litem* comparable à celui des avocats, de sorte que les développements consacrés *supra* aux avocats leur sont dans une grande partie applicable. Ils interviennent au nom et pour le compte des membres de l'organisation à laquelle ils appartiennent et sont habilités à engager leurs affiliés par le dépôt et la communication d'actes de procédure (requête, conclusions…).

[89] Art. 549 à 555 du Code judiciaire.
[90] A. FETTWEIS, *Manuel de procédure civile*, Faculté de droit de Liège, 1987, pp. 389-390.

Tout comme les avocats, ils doivent être titulaires de signature électronique avancée appuyée par un certificat qualifié établi au nom de la personne physique qui, au sein de l'organisation représentative, est habilitée à engager le travailleur et à le représenter en justice. Il s'agira, le plus généralement, du responsable juridique de l'organisation ou de l'un de ses délégués.

Le certificat dont ils doivent disposer mentionnera leur identité complète ainsi que l'organisation (association de fait) à laquelle ils appartiennent.

e) Notaires

La profession de notaire est réglementée par la loi du 25 ventôse an XI contenant organisation du notariat telle que modifiée par la loi du 4 mai 1999[91].

Sans empiéter sur les questions spécifiques relatives à l'acte authentique électronique ainsi qu'à l'archivage étudiées ci-après (chapitres II et III), notons que les notions d'authentification notariale et de certification sont différentes même si parfois complémentaires. L'authentification du notaire entend garantir le contenu d'un acte et de la réalité de l'adhésion des parties à celui-ci sur base d'un consentement libre et éclairé. La certification électronique ne porte, quant à elle, que sur la signature. Les PSC se limitent à vérifier l'identité des titulaires de clés publiques et à créer et délivrer des certificats, mais n'authentifient jamais le contenu des actes signés électroniquement[92]. Quant à l'enregistrement, il consiste à collecter les données destinées à figurer sur le certificat de façon fiable et sécurisée.

Concernant l'attribution de signatures électroniques aux notaires, la Chambre nationale des notaires[93] et/ou les compagnies provinciales ont vocation à devenir l'autorité d'enregistrement[94].

A terme, selon un raisonnement identique à celui tenu à l'endroit des huissiers et des avocats, il ne serait pas surprenant de voir les notaires investir eux aussi la sphère de l'activité de l'enregistrement et délivrer à leur tour des certificats à leurs clients (par l'entremise d'un PSC se chargeant de l'attribution technique des clés).

4. Justiciables

Les justiciables, personnes physiques ou morales, qu'ils agissent en qualité de demandeurs ou de défendeurs, devront également recourir à la signature électronique pour signer valablement l'ensemble des actes de procédure pour lesquels leur signature est exigée.

Une fois encore, les exigences de validité ne seront valablement remplies que pour autant que les justiciables disposent de certificats qualifiés et de signatures électroniques avancées.

Ces certificats reprendront l'identité complète des signataires.

---

[91] Loi du 4 mai 1999 modifiant la loi du 25 ventôse an XI portant organisation du notariat, *Mon. b*. 1er oct. 1999

[92] D. GOBERT, E. MONTERO, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *J.T.*, n°6000, Larcier, Bruxelles, p. 123.

[93] Art. 90 et s. de la loi du 16 mars 1803 contenant organisation du notariat.

[94] Y. TIMMERMANS, "Signature électronique et certification : le notariat et les nouvelles technologies", in *Signature électronique et certification*, Actes du colloque, L.L.N., 25 sept. 2001, p. 6.

Signalons que les justiciables peuvent intervenir en justice par l'intermédiaire de tiers. Si l'on sait que les avocats bénéficient du monopole de la plaidoirie et du droit de représentation, notons qu'il existe d'autres personnes susceptibles d'intervenir en justice au nom et pour le compte de justiciables. Nous songeons notamment aux apparentés (qui peuvent, dans certaines circonstances représenter leur parent), aux tuteurs (légaux ou ad hoc), aux administrateurs…

Ces derniers devront bien évidemment disposer également de certificats qualifiés et de signatures électroniques avancées indiquant leur identité complète.

Concernant les personnes morales, en ce qui concerne la responsabilité liée à l'usage de la signature électronique de la personne morale par une personne physique habilitée, le Ministre questionné par un membre de la commission du Sénat, a fait savoir que c'était la personne morale qui était responsable[95]. Cette détermination de la personne responsable n'est pas contradictoire avec l'obligation imposée aux PSC par le paragraphe 3 de l'article 8 (modifié par le Sénat) de tenir un registre reprenant les noms et qualités de la personne physique habilitée à signer électroniquement pour une personne morale[96].

Il est à noter à ce propos qu'il ressort du rapport établi par la commission de la Chambre que le Ministre a encore précisé qu'une personne morale ne pouvait être représentée "que par une seule personne physique faisant usage de la signature électronique"[97]. Les registres tenus par les PSC ne pourront donc indiquer qu'une seule personne physique habilitée à faire usage de la signature électronique de la personne morale.

Cette formulation est malheureuse. En effet, s'il est clair qu'un certificat relatif à une personne morale ne peut être attribué qu'à une seule personne physique, il ne fait aucun doute dans le même temps qu'une personne morale pourra être représentée par différentes personnes physiques, chacune titulaire d'un certificat émis au nom de la personne morale mais rattaché à une fonction propre dans la société. Ainsi, l'usage de la signature électronique par les personnes morales demeure possible dans toutes les hypothèses où des dispositions législatives ou réglementaires exigent plus d'une signature pour engager valablement la personne morale (nous pensons notamment à certaines dispositions relatives aux sociétés commerciales).

[95] Projet de loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, Rapport fait au nom de la commission des finances et des affaires économiques par Monsieur STEVERLYNCK, *Doc. Parl*., Sénat, 2000-2001, 8 mai 2001, 2-662/5.

[96] Projet de loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, Rapport fait au nom de la commission de l'économie, de la politique scientifique, de l'éducation, des institutions scientifiques et culturelles nationales, des classes moyennes et de l'agriculture, *Doc. Parl*., Ch. Repr., sess. Ord. 2000-2001, 6 juin 2001, n°322/007, p. 3.

[97] Projet de loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, Rapport fait au nom de la commission de l'économie, de la politique scientifique, de l'éducation, des institutions scientifiques et culturelles nationales, des classes moyennes et de l'agriculture, *Doc. Parl*., Ch. Repr., sess. Ord. 2000-2001, 6 juin 2001, n°322/007, p. 3.

IV. CONCLUSIONS, RECOMMANDATIONS ET PERSPECTIVES

"Dans un réseau ouvert, en l'absence de sécurité issue de l'architecture du réseau, la sécurisation doit s'opérer sur l'information elle-même"[98]. La justice électronique prenant place dans un univers dématérialisé, la confiance des intervenants en un système virtuel s'avère être l'une des clés de la réussite du système.

Or, comment susciter et garantir cette confiance dès lors que, d'une part, l'ensemble de l'appareil judiciaire et de la procédure, élaborés pour et autour du papier, s'avère *prima facie* sous certains aspects peu compatible avec certaines des caractéristiques propres aux NTIC et que, d'autre part, l'échange de données par voie électronique ne manque pas de susciter certaines interrogations quant au niveau de sécurité des systèmes utilisés.

Comment garantir la pérennité des données ou leur intégrité, l'identité des parties en présence, l'imputabilité des messages envoyés, la confidentialité dans l'échange des données, la réception effective du message permettant de garantir sa non répudiation ainsi que l'horodatage des données transmises ?

Certes la certification permet d'apporter des réponses à plusieurs de ces questions, parmi lesquelles les épineuses mais essentielles exigences en matière d'identification et de garantie d'intégrité et d'imputabilité des messages : l'utilisation croisée d'un certificat qualifié et d'une signature électronique avancée permet, dans une large mesure, de répondre à cette exigence de sécurisation des données elles-mêmes. Dans la plupart des cas, et sous réserve d'hypothèses particulières, l'attribution de certificats et de mécanismes de signature électronique ne devrait pas susciter de difficultés particulières : les membres de professions réglementées accéderont le plus vraisemblablement à la signature électronique par l'intermédiaire de leurs autorités professionnelles (ordre, chambre nationale, fédération…), les titulaires d'autres professions disposeront le cas échéant de moyens de signature par l'entremise d'une inscription sur une liste par une commission (mandataires judiciaires, commissaires aux comptes...), tandis que les membres de la fonction publique devraient, à terme, idéalement, disposer de clés publiques uniformisées à un niveau fédéral. Les simples justiciables (personnes physiques) devront quant à eux souscrire directement auprès d'un PSC l'attribution d'une signature électronique authentifiée par certificat. Pareille démarche, bien qu'elle puisse paraître aujourd'hui encore quelque peu éloignée à beaucoup, rentrera très certainement dans les usages, des entreprises dans un premier temps, des particuliers ensuite.

De même la cryptographie permet-elle de répondre aux nécessités de confidentialité : la cryptographie asymétrique permet d'assurer, par le chiffrement au moyen d'algorithmes, la conversion d'un message en un ensemble de données inintelligibles pour toute autre personne que le destinataire.

Mais certaines questions demeurent ouvertes et les difficultés se dévoilent au fur et à mesure que se dessine le tableau d'ensemble d'une architecture à clés publiques conforme aux principes et objectifs de la justice.

[98] E. DAVIO, "Preuve et certification sur internet", *R.D.C.*, 1997, pp. 660-670.

Parmi celles-ci, la question de l'interopérabilité des systèmes utilisés s'avère être l'une des questions fondamentales, et des plus ardues[99]. Comment en effet assurer la compatibilité de systèmes qui, on l'a vu, seront le plus généralement issus d'initiatives privées et éparses ? Par exemple, comment assurer que le système de signature électronique privilégié par l'Ordre des avocats francophones de Bruxelles soit compatible avec celui que sélectionnera le monde judiciaire pour les magistrats et les greffiers ? Quels standards techniques faudra-t-il élaborer ? Quelle qualité de clés convient-il de favoriser ?

A titre de proposition de solution, il nous semble que l'élaboration d'un régime général de certification pour les différents intervenants de la Justice ne pourrait être dissociée des différents travaux menés par ailleurs par le gouvernement fédéral dans l'élaboration d'une infrastructure à clés publiques fédérale visant à l'attribution de clés publiques aux membres de l'administration (FedPKI)[100].

Ce projet, tendant à la détermination des moyens techniques et juridiques nécessaires pour l'informatisation de l'administration en général, pose les bases d'une uniformisation des standards techniques de certification pour l'administration fédérale (carte d'identité électronique, portails gouvernementaux, messagerie uniformisée…) et poursuit notamment l'objectif de mettre en place une infrastructure à clés publiques (ICP – PKI) basée sur un système d'authentification et d'autorisation sécurisées. L'élaboration de cette ICP, non exempte d'une certaine dimension juridique, ne pourra, à terme, faire l'économie d'une réflexion sur la nécessité ou non de doter cette ICP d'un statut officiel fixé par la loi, outre les dispositions relatives à la certification[101]. A ce propos, la CNUDCI considère que la coexistence de deux types d'infrastructures (l'une avec un fondement légal, l'autre non) sera, en raison des initiatives privées grandissantes et en l'absence de réglementation, une réalité d'ici quelques années[102].

Cette question renvoie à la détermination du rôle de l'Etat, à la fois prescripteur, régulateur et utilisateur.

La question de l'équipement s'avère être une seconde pierre d'achoppement d'importance. Il ne sert à rien en effet de déterminer les critères réglementaires devant entourer la sécurisation de l'échange de données par voie informatique ainsi que la certification du contenu et des acteurs si l'ensemble de ces mêmes acteurs ne disposent pas de l'équipement nécessaire et adéquat pour conférer à l'informatisation de la justice une effectivité au moins aussi satisfaisante que celle garantie par l'administration traditionnelle de la justice.

Ces problèmes sont essentiellement d'ordre technique et ne pourraient en aucun cas justifier un quelconque désintérêt à l'égard de l'e-Justice, mais constituent néanmoins des obstacles importants à un développement rapide et efficace de la justice électronique.

---

[99] Soulignons à cet égard l'initiative de huit partenaires du monde bancaire et de la certification en Belgique qui ont fondé ECERTIO, dont l'ambition est d'être un producteur 'industriel' à l'échelle européenne de certificats électroniques. Pour info, voy. http://www.ecertio.com

[100] Pour plus de détails quant au plan fédéral d'élaboration d'une infrastructure à clés publiques, voyez "FedPKI : The Belgian Federal Government's internal PKI-environment", document de travail rendu public, disponible sur le site de la Fedict : http://www.fedict.be

[101] Voyez à ce propos B. BRADFORD, *Public Key infrastructure and digital signature legislation : ten public questions*, *Cyberspace Lawyer*, 1997, vol. 2, n°2.

[102] Voy. le rapport du groupe de travail sur le commerce électronique, 31ème session, New York, 18-28 février 1997, A/CN.9/437, 12 mars 1997.

Enfin, un autre aspect important dans le cadre de la certification des acteurs et du contenu des actes à caractère juridique réside dans le financement d'une telle opération. Si le coût total des aménagements nécessaires à la mise en place d'une plate-forme efficiente de justice électronique s'avère difficile à évaluer, il demeure que les coûts liés à l'octroi d'un certificat et d'un mécanisme de signature électronique reposeront, pour la grosse majorité, sur les acteurs eux-mêmes. Or, ces acteurs seront-ils toujours en mesure de disposer de ces moyens ? Nous pensons essentiellement aux justiciables (personnes physiques), qui constituent la part la plus importante des destinataires de justice. La généralisation de l'utilisation de documents électroniques nécessite au préalable la généralisation des moyens techniques de sécurisation.

CHAPITRE II

LA CONSERVATION ET LA DATATION DES DOCUMENTS ELECTRONIQUES

Table des matières

CHAPITRE II

LA CONSERVATION ET LA DATATION DES DOCUMENTS ELECTRONIQUES

INTRODUCTION : OBJET ET LIMITES DU PRÉSENT CHAPITRE

L'intégration des nouvelles technologies de l'information et de la communication dans notre société entraîne la multiplication des documents sous forme électronique. Or, nombre de ces documents doivent être conservés à plus ou moins long terme, pour différentes raisons. Se pose alors la question incontournable de leur archivage électronique, dans un monde dématérialisé, face à une technologie en perpétuelle évolution.

Si la conservation de documents est déjà envisagée par le législateur depuis longtemps, les problèmes posés par l'avènement des nouvelles technologies n'ont pas fait l'objet, à ce jour, d'une intervention législative en cette matière, à quelques rares exceptions près[103]. En outre, un rapide tour d'horizon a tôt fait de démontrer que l'archivage électronique au sens large concerne de nombreuses branches du droit et de nombreux acteurs, tant privés que publics, avec des intérêts, des priorités et des exigences différents.

La conservation de documents peut trouver sa source tant dans une obligation légale que dans une nécessité pratique. Il peut s'agir d'une obligation de conservation à des fins de contrôle ou afin d'assurer le bon fonctionnement du service public, mais aussi d'une obligation *ou* d'une nécessité de conserver à des fins probatoires. D'autres motifs sont également envisageables, mais étrangers à la présente étude : gestion efficace, fonctionnement interne, préservation d'un patrimoine historique ou culturel…

D'une part, c'est la conservation de documents à des fins probatoires qui retient d'emblée notre attention (I). D'autre part, nous examinons l'obligation légale de conservation, sous l'angle des professions juridiques (II). Dans le premier comme dans le second cas, il convient de déterminer les conditions strictes d'une conservation fiable dans l'environnement numérique (III). On se penche également sur la datation des documents dans un contexte numérique, cette question étant souvent étroitement liée à celle de la conservation (IV). Enfin, l'étude se termine par quelques recommandations et propositions de textes législatifs en matière de conservation de documents électroniques (V).

[103][103] Voy., par exemple, l'art. 60 du Code de la TVA et l'art. 315*bis* du C.I.R.

Remarque préliminaire : précisions terminologiques

Les auteurs s'accordent pour distinguer l'archivage de la conservation[104].

Le terme 'archivage' est relatif à la science archivistique et porte sur des méthodes en vue de conserver des documents, quels qu'ils soient : modalités pratiques, choix du support, méthodes de tri et de classement. L'archivage viserait donc l'aspect technique, voire physique, de la question.

Le terme 'conservation', quant à lui, s'attache au contenu juridique du document archivé. Il s'agit de " maintenir intacts les documents et de les préserver de toute altération, modification ou destruction (…) de façon à assurer la sauvegarde d'un droit "[105].

A l'évidence, archivage et conservation sont intimement liés, l'un n'allant pas sans l'autre.

Dans la présente étude, le terme 'document' désigne tout type d'information susceptible d'être conservé : actes, pièces, registres, dossiers, conclusions, courriers, etc.

[104] E. CAPRIOLI, "Variations sur le thème du droit de l'archivage dans le commerce électronique", *Petites affiches*, 18 août 1999, p. 4-5 ; T. PIETTE-COUDOL, *Echanges électroniques, certification et sécurité*, Paris, Litec, 2000, p. 197 ; J.-L. SNYERS, "De elektronische, authentieke akte en de notariële, elektronische archivering", *Limb. Rechts*, 2000, p. 293.
[105] G. CORNU, *Vocabulaire juridique*, Paris, P.U.F., 1996, V° Conservation, p. 196.

I. LA CONSERVATION DE DOCUMENTS À DES FINS PROBATOIRES

La conservation de certains documents peut être motivée par la nécessité de se préconstituer des preuves en cas de litige. Ainsi, lorsqu'il s'agit d'un acte juridique ayant fait naître des droits et des obligations, tel un contrat, la production de ce document permettra de fournir la preuve de l'existence d'un droit ou de l'exécution d'une obligation, et de prévenir ou de régler les éventuelles contestations[106].

Se pose alors l'incontournable question de la valeur probante des documents électroniques, au regard des concepts fondamentaux du droit de la preuve (A). Quant à la durée de conservation de ces éléments de preuve, elle est intimement liée à la question de la prescription (B).

A. Le problème de la valeur probante d'un document électronique

La question primaire et incontournable lorsqu'on aborde la conservation de documents électroniques est celle de leur valeur probante. En effet, rien ne sert d'envisager les modalités de conservation de tels documents si leur production en justice n'est pas reconnue. Il convient dès lors d'examiner la valeur des documents numériques issus des nouvelles technologies sous l'angle des concepts fondamentaux du droit de la preuve.

L'ensemble des notions du droit de la preuve ne fait pas l'objet de ce rappel dans la mesure où certaines d'entre elles n'ont aucune pertinence au regard du sujet traité. Ceci dit, il paraît primordial d'examiner les quelques règles du Code civil en matière probatoire. On se penche d'abord sur le principe de la prééminence de l'écrit (1) et ses exceptions (2), avant d'aborder la reconnaissance légale de la signature électronique (3). La nécessité d'une définition légale de l'écrit est ensuite envisagée, accompagnée de propositions de textes (4). Ce tour d'horizon de notre droit de la preuve s'achève sur les notions d'original et de copie, incontournables lorsqu'on aborde la question de la conservation et de la reproduction de documents électroniques (5).

1. Le principe de la prééminence de l'écrit : conséquences en droit de la preuve

Notre système probatoire est fondé sur le principe de la prééminence de l'écrit signé : la preuve absolue est la preuve écrite[107]. Un auteur expliquait cette faveur reconnue à l'écrit signé " par la haute valeur sécuritaire de l'écrit, caractérisé par sa permanence, par une signature dans laquelle l'auteur se reconnaît et parce qu'il apparaît comme un support efficace à l'information des parties "[108].

Le fondement juridique de ce principe réside dans l'article 1341 du Code civil, qui dispose : "*Il doit être passé acte devant notaire ou sous signature privée, de toutes choses excédant une somme ou valeur de 15.000 francs*". En d'autres mots, la partie qui veut établir

---

[106] Notons que cette conservation à des fins probatoires peut être volontaire, car motivée par la prudence, ou être imposée par la loi. En effet, nombre d'obligations légales de conservation poursuivent notamment un objectif probatoire, dans un souci de sécurité juridique, afin d'éviter la multiplication de litiges (*infra*, point II).

[107] Pour une étude approfondie des principes, voy. R. MOUGENOT, *Droit des obligations : La preuve*, Larcier, 1997, 2e édition, pp. 98 et s. ; N. VERHEYDEN-JEANMART, *Droit de la preuve*, Précis de la Faculté de Droit de l'Université Catholique de Louvain, Bruxelles, Larcier, 1991, pp. 234 et s.

[108] Y. POULLET, "Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve", in *Le droit des affaires en évolution, Le juriste face à l'invasion informatique*, Colloque ABJE, 24 oct. 1996, Bruxelles, Bruylant, Anvers, Kluwer, 1996, p. 48. Remarquons que cette vision des choses doit être considérablement nuancée au regard des développements technologiques récents (cf. *infra*).

l'existence d'un acte juridique en matière civile[109], dont la somme dépasse 15.000 francs belges[110], doit en apporter la preuve par un écrit signé[111]. Il en résulte qu'en l'absence d'un tel écrit, l'acte juridique existe mais ne peut être prouvé.

La question fondamentale au regard des nouvelles technologies est de savoir ce qu'on entend par " écrit signé ". En effet, de la réponse à cette question dépendra l'extension de cette notion aux documents signés électroniquement (tel un e-mail signé digitalement). Or, à l'heure actuelle, la question reste ouverte, la loi ne donnant pas de définition de la notion d'écrit (voy. *infra*, point 4). Quant à la notion de signature, jusqu'à la loi du 20 octobre 2000[112], le Code civil n'en donnait pas non plus de définition[113] (voy. *infra*, point 3).

Auparavant, la jurisprudence constante de la Cour de cassation[114] et une partie de la doctrine[115] belge palliaient cette carence en envisageant l'écrit en relation avec un support papier et en définissant la signature comme devant être un signe, accompagné d'un certain graphisme, apposé de manière manuscrite. Cette conception est aujourd'hui dépassée, avec l'adoption récente de la loi du 20 octobre 2000.

2. Exceptions au principe de la prééminence de l'écrit

Malgré la conception très formaliste qui avait été donnée aux notions d'écrit et de signature (avant l'adoption de la loi du 20 octobre 2000), rien n'interdisait d'exploiter les exceptions au principe de la prééminence de l'écrit ou d'exploiter le caractère supplétif des règles de preuve, même si le recours aux exceptions ne constitue pas la panacée[116]. On sait également qu'en matière commerciale, la preuve est libre et que dès lors la présentation d'un écrit signé pour faire preuve n'est pas exigée, même si la somme dépasse 15.000 francs belges. Il en va de même pour la preuve des faits juridiques.

---

[109] En matière commerciale, la preuve est libre (art. 25, al. 1er, C. comm. et art. 1341, al. 2, C. civ.

[110] 371,84 euros.

[111] Ce qui exclut la preuve par témoignages et présomptions, sauf si la partie peut se prévaloir des exceptions à l'article 1341, à savoir l'article 1347 (commencement de preuve par écrit) ou l'article 1348 (impossibilité de se procurer un écrit).

[112] Loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 décembre 2000, pp. 42698 à 42699. Par souci de clarté de l'exposé, nous traiterons du contenu de cette loi dans un titre spécifique à la signature.

[113] Toutefois, avant l'adoption de ce texte, la position selon laquelle le Code civil n'excluait pas la signature électronique était déjà défendue : civ. Namur, 25 juin 1990, *R.R.D.*, 1992, pp. 60 et s. Pour un commentaire, voy. D. GOBERT, " La sécurisation des échanges par la reconnaissance de la signature électronique : condition d'existence des réseaux d'avocats ", in *Multimédia: Le cyberavocat*, Formation permanente CUP, Volume XXIX, Liège-Namur, février 1999, p. 173. X. THUNIS en conclut même que la " notion d'écrit signé peut s'interpréter assez largement étant donné l'imprécision ou l'ouverture providentielle des concepts fondamentaux, écrit et signature ", X. THUNIS, *Responsabilité du banquier et automatisation des paiements*, Travaux de la Faculté de droit de Namur, P.U.N., 1996, p. 228 et les références citées aux notes 67 et 68.

[114] Cass., 24 févr. et 3 nov. 1910, *Pas.*, 1910, I, pp. 241 et 475 ; Cass., 1er mars 1917, *Pas.*, 1917, I, p. 118; Cass., 7 janv. 1955, *Pas*., 1955, I, p.456 ; Cass., 2 oct. 1964, *Pas*., 1965, I, p. 106 ; Cass., 28 juin 1982, *R.C.J.B.*, 1985, p. 69, note M. VAN QUICKENBORNE.

[115] Voir par exemple E. DUBUISSON qui considère que la signature numérique ne constitue pas l'équivalent de la signature manuscrite : " La personne virtuelle : proposition pour définir l'être juridique de l'individu dans un échange télématique ", *D.I.T.*, 1995/3, p. 8 ; M. VAN QUICKENBORNE, " Quelques réflexions sur la signature des actes sous seing privé ", note sous Cass. 28 juin 1982, *R.C.J.B.*, 1985, p. 69.

[116] Y. COOL, " Signature électronique et signature manuscrite: sœurs ennemies ou sœurs jumelles ? ", in *Droit des technologies de l'information. Regards prospectifs* (sous la direction de E. MONTERO), Cahiers du CRID, n° 16, Bruxelles, Bruylant, 1999, p. 80.

a) Le commencement de preuve par écrit

L'article 1347 dispose que : "*Les règles ci-dessus reçoivent exception lorsqu'il existe un commencement de preuve par écrit. On appelle ainsi tout acte par écrit qui est émané de celui contre lequel la demande est formée (…) et qui rend vraisemblable le fait allégué.* "

La question qui se pose est de savoir si le document signé électroniquement entre dans cette définition et, si oui, si cela peut aider à résoudre le problème.

Les conditions pour constituer un commencement de preuve par écrit sont clairement définies. Or, deux de celles-ci semblent poser difficulté.

Tout d'abord, il faut un acte écrit, c'est-à-dire "sous une forme littérale quelconque "[117]. Cette conception va-t-elle jusqu'à admettre un acte électronique ? Cela n'est pas certain, même si selon nous, on devrait pouvoir admettre qu'un téléfax, un enregistrement magnétique[118], un télex, un e-mail ou la page d'un site web[119] constituent un acte par écrit au sens de l'article 1347 du Code civil. Ici encore, tout dépend de l'interprétation qui est donnée de la notion d'écrit.

Ensuite, il appartient au juge d'apprécier souverainement, au cas par cas, si l'acte rend vraisemblable le fait allégué[120], donc sa valeur probante. Dans ce contexte, on comprend qu'une insécurité juridique subsiste.

Enfin, notons que le commencement de preuve par écrit ne fait qu'ouvrir la voie aux autres modes de preuve (témoignage et/ou présomption). On le voit, le problème n'est pas encore résolu quand on a établi qu'il y avait commencement de preuve par écrit.

b) L'impossibilité de se constituer un écrit

L'article 1348 du Code civil dispose que *" [Les règles ci-dessus] reçoivent encore exception toutes les fois qu'il n'a pas été possible au créancier de se procurer une preuve littérale de l'obligation qui a été contractée envers lui. "* Cette impossibilité peut être de trois types : morale, matérielle ou résultant des usages[121]. Ce sont ces deux derniers cas qui nous intéressent.

- L'impossibilité matérielle

Cette première exception concerne les cas où l'on ne peut raisonnablement attendre des parties qu'elles préconstituent une preuve écrite, eu égard aux circonstances exceptionnelles entourant la création de l'acte en question[122]. La jurisprudence interprète cette règle de

[117] Cass., 21 oct. 1891, *Pas.*, 1892, I, p. 58. Le lecteur sera attentif au fait que "l'acte par écrit" visé à l'article 1347 ne doit pas s'entendre comme un écrit signé mais seulement comme un simple écrit.
[118] D. MOUGENOT, " Droit de la preuve et technologies nouvelles: synthèse et perspectives ", *Droit de la preuve-Formation permanente CUP*, Volume XIX, octobre 1997, p. 83.
[119] E. DAVIO, " Preuve et certification sur Internet ", *R.D.C.*, 1997, n° 11, p. 664.
[120] Cass., 21 oct. 1891, *Pas.*, 1892, I, p. 58.
[121] H. DE PAGE, *Traité élémentaire de droit civil belge*, t. 3, Bruxelles, Bruylant, n° 901.
[122] M. FONTAINE, " La preuve des actes juridiques et les techniques nouvelles ", in *La Preuve*, colloque U.C.L., 1987, p. 18.

manière stricte en exigeant " une véritable impossibilité et non de simples difficultés "[123]. Il semble donc malaisé de faire application de cette exception dans notre cas. Comme le fait remarquer le professeur Y. POULLET, " L'impossibilité de prouver par écrit est une exception dont le maniement apparaît difficile, au moment où c'est volontairement que celui qui se prévaudrait de cette exception s'est privé de cet écrit "[124].

L'insécurité juridique subsiste puisqu'il est impossible d'anticiper la décision des tribunaux sur l'applicabilité ou non de cette exception.

- L'impossibilité résultant des usages

Ce type d'impossibilité vise des situations de la vie courante dans lesquelles "il n'est pas d'usage, car la chose serait impraticable"[125] d'établir un acte écrit. L'on pense par exemple aux billets de spectacle, ou aux repas au restaurant, dont les montants dépasseraient quinze mille francs. Le raisonnement se base sur les désagréments pratiques que susciterait la constitution d'un acte écrit.

Si l'utilisation de cette exception paraît plus plausible, le système qui se mettrait en œuvre ne serait néanmoins guère satisfaisant. La reconnaissance d'une impossibilité ne fait qu'ouvrir la voie aux autres modes de preuve. La preuve reste donc difficile à apporter. De plus, la signature électronique ne serait pas reconnue en tant que telle, au même titre qu'une signature manuscrite, avec les avantages que cela présente.

c) Les limites de la voie conventionnelle en réseau ouvert

Pour trouver une solution à ces problèmes, la voie conventionnelle s'est imposée naturellement dans le contexte des réseaux fermés (de banque à distance ou d'EDI[126]), grâce à l'incontestable caractère supplétif des dispositions légales relatives à la preuve. En effet, les contractants ne se privent pas de fixer leurs propres règles probatoires dans un " contrat papier ", s'accordant notamment pour assimiler la signature électronique à la signature manuscrite. Cependant, cette solution, qui exige des rapports préalables et suivis entre parties, n'est guère adaptée aux réseaux ouverts, tel l'internet, où chacun peut nouer des contacts et conclure des actes juridiques avec des partenaires occasionnels[127].

d) Le régime de la preuve libre

On le sait, lorsqu'on fait la preuve d'un acte juridique inférieur à 15.000 francs belges ou à l'égard d'un commerçant, la preuve est libre. Il en est de même pour la preuve des faits juridiques. Dans ce régime, tout mode de preuve est recevable. Cela signifie qu'un document signé électroniquement sera admissible comme moyen de preuve par le juge. Mais cela n'est

---

[123] M. ANTOINE et D. GOBERT, " Pistes de réflexion pour une législation relative à la signature électronique et au régime des autorités de certification ", *R.G.D.C.*, 1998, 4/5, p.290. Pour plus de détails, voir aussi P. WÉRY, note sous Liège, 10 mars 1994, *J.M.L.B.*, 1994, pp. 894 et s.

[124] Y. POULLET, *op. cit.*, p. 43.

[125] M. FONTAINE, *op. cit.*, p. 18.

[126] Tels que SWIFT ou ISABEL (réseaux interbancaires), ASSURNET (dans le secteur des assurances), ODETTE (secteur automobile), GALILEO ou AMADEUS (agences de voyages).

[127] D. GOBERT et E. MONTERO, " La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle ", *in Commerce électronique : le temps des certitudes*, Cahiers du CRID n° 17, Bruxelles, Bruylant, 2000, pp. 53-97.

guère satisfaisant. En effet, être recevable n'implique pas, loin s'en faut, d'avoir une valeur probante. Le pouvoir discrétionnaire du juge demeure[128], et l'insécurité juridique subsiste.

3. La reconnaissance légale de la signature électronique

Jusqu'à la loi du 20 octobre 2000, une conception formaliste de la signature avait été donnée par la jurisprudence et une partie de la doctrine, ce qui avait pour effet de réduire celle-ci à la signature manuscrite (cf. *supra*). Cette vision des choses, aujourd'hui dépassée, n'avait toutefois pas empêché certains auteurs de mettre en avant une conception plus fonctionnelle de la signature, estimant que pouvait constituer une signature tout mécanisme qui remplit la double fonction assignée traditionnellement à celle-ci, à savoir identifier l'auteur d'un acte et exprimer son adhésion au contenu de ce dernier[129].

Depuis la loi du 20 octobre 2000, notre Code civil contient une disposition spécifique relative à la signature. Ainsi, le nouvel alinéa 2 de l'article 1322 du Code civil, introduit par l'article 2 de la loi précitée, stipule que "*Peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte*"[130].

Sans entrer dans une analyse approfondie de cette disposition[131], il s'agit assurément d'une définition fonctionnelle de la signature. Pour faire le lien avec la directive européenne relative à la signature électronique, nous pouvons dire qu'elle vise la clause de non discrimination prévue à l'article 5 de celle-ci[132]. Cette définition de la signature permet ainsi de consacrer le principe de la *recevabilité* de tout type de signature électronique, le juge étant alors libre, dans les limites toutefois des conditions de l'article 1322, al. 2, d'apprécier la valeur probante à accorder dans chaque cas. En d'autres mots, soit il considère que les fonctions d'imputabilité et de maintien de l'intégrité sont remplies avec une certitude raisonnable, et dans ce cas, il accorde nécessairement une valeur probante équivalente à celle de la signature manuscrite, ce qui signifie que l'écrit signé électroniquement constitue un acte sous seing privé au sens de l'article 1341 du Code civil ; soit le juge considère que le mécanisme qui lui est présenté ne remplit pas les fonctions, et dès lors, il considère que le document n'est pas signé. Le cas échéant, l'écrit électronique peut néanmoins constituer un commencement de preuve par écrit ou une copie[133] par exemple.

---

[128] M. ANTOINE et D. GOBERT, *op. cit.*, p. 289.

[129] Pour un exposé détaillé sur la question, voy. D. GOBERT et E. MONTERO, " La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle ", *DA/OR, op. cit.*, pp. 17-39.

[130] On peut regretter que la nouvelle mouture de l'article 1322, al. 2, n'exige plus que la signature électronique suppose une transformation de l'écrit. En effet, dans le projet de loi originaire, il était nécessaire que l'ensemble de données soit le résultat d'une transformation, quelle qu'elle soit, de l'écrit, de sorte que s'établisse un lien indissociable entre l'écrit et la signature, sans quoi on ne peut être sûr que c'est cet écrit qui émane du prétendu signataire. Sur l'importance du lien indissociable entre la signature et l'écrit électronique, voy. D. GOBERT et E. MONTERO, *DA/OR, op. cit.*, p. 37. Voy. aussi D. GOBERT et E. MONTERO, " L'ouverture de la preuve littérale aux écrits sous forme électronique ", *J.T.*, n° 6000, pp. 117-119.

[131] Pour plus de détails, voy. P. LECOCQ et B VANBRABANT, " La preuve du contrat conclu par voie électronique " *in Le commerce électronique : un nouveau mode de contracter ?*, Editions du jeune barreau de Liège, 2001, pp. 112 et s. ; M. E. STORME, " De invoering van de elektronische handtekening in ons bewijsrecht – Een inkadering van en commentaar bij de nieuwe wetsbepalingen ", *R.W.*, 9 juin 2001, n° 41, pp. 1505-1525 ; D. GOBERT et E. MONTERO, " L'ouverture de la preuve littérale aux écrits sous forme électronique ", *J.T.*, n° 6000, pp. 119-120.

[132] Pour plus de détails, voy. M. ANTOINE et D. GOBERT, " La directive européenne sur la signature électronique : vers la sécurisation des transactions sur l'Internet ? ", *J.T.D.E.*, 2000, n° 68, pp. 73-78 .

[133] Ce serait le cas pour un original papier qui serait scanné. Le fichier "image " qui en résulte constitue une copie de l'original au format papier.

Selon cet article, il ne fait nul doute que tout type de signature doit désormais être déclaré recevable par le juge. Il n'est donc plus possible de contester un document signé électroniquement au seul motif que la signature n'est pas manuscrite. Le juge devrait en outre théoriquement prendre le temps de vérifier si les fonctions (imputabilité et maintien de l'intégrité) sont remplies pas le mécanisme présenté et, sur cette base, se prononcer sur la valeur probante qu'il lui accorde. Il appartiendrait dans ce cas à celui qui se prévaut de l'acte signé d'administrer cette preuve.

Il semble néanmoins que le juge devrait dispenser la partie de cette preuve difficile, et surtout se dispenser d'un tel examen, lorsque l'acte signé n'est pas contesté par le signataire (même si la signature est sommaire ou réalisée à l'aide d'un mécanisme peu sécurisé). L'absence de contestation pourrait être interprétée comme une approbation par le signataire du contenu de l'acte et comme une ratification qu'il émane effectivement de lui[134], et donc comme une preuve automatique que les fonctions sont remplies.

Par ailleurs, l'article 4, § 4, de la loi du 9 juillet 2001fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification[135] dispense le juge de vérifier si les deux fonctions précitées sont remplies lorsqu'il a affaire à "une signature électronique avancée réalisée sur base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique ". En effet, une telle signature est désormais assimilée par la loi à une signature manuscrite.

L'article 1322, al. 2, du Code civil est applicable à tous les actes sous seing privé, pour autant qu'ils ne soient pas soumis à une législation spécifique. Il en résulte que si une loi prévoit des dispositions particulières faisant obstacle à l'utilisation de la signature électronique, ces dispositions devront être respectées tant que la législation spécifique n'aura pas été adaptée. A cet égard, certains auteurs se sont inquiétés de ce que l'article 1322, al. 2, ne concernait que le domaine de la preuve des obligations et que, partant, il ne transposait pas adéquatement la directive sur la signature électronique, qui a un champ d'application plus large[136].

Il nous semble que ces craintes devraient pouvoir être apaisées par l'adoption d'une disposition adéquate dans le cadre de la transposition de la directive sur le commerce électronique[137], et spécialement son article 9. En effet, afin de lever les obstacles (directs et indirects) à la conclusion de contrats par voie électronique, le législateur devrait adopter une disposition générale, stipulant que chaque fois qu'une disposition légale ou réglementaire exige (à des fins probatoires ou autres) une signature, cette exigence est satisfaite même si la signature est électronique, pour autant que soient respectées les conditions de l'article 1322, al. 2, nouveau du Code civil et de l'article 4, § 4, de la loi sur les prestataires de service de certification[138]. Les récents travaux menés sur la transposition de la directive sur le commerce électronique s'orientent précisément dans cette direction.

---

[134] D. GOBERT et E. MONTERO, *DA/OR, op. cit.*, p. 37.
[135] *M.B.*, 29 sept. 2001.
[136] P. LECOCQ et B VANBRABANT, *op. cit.*, p. 127.
[137] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("directive sur le commerce électronique", ci-après "la directive"), *J.O.C.E.*, n° L 178 du 17 juillet 2000, p. 1.
[138] En ce sens, D. GOBERT et E. MONTERO, "Le traitement des obstacles formels aux contrats en ligne", Cahiers du CRID, n°19, *op. cit.*, pp. 199 à 244. Dans le même ouvrage, voyez la proposition de disposition législative en annexe, art. 17, § 2, al. 4, p. 418.

La modification adoptée ne semble viser que les actes sous seing privé, à l'exclusion des actes authentiques. En effet, ni les dispositions de la loi du 20 octobre 2000, ni son exposé des motifs, ne traitent de l'acte authentique[139]. De plus, la définition fonctionnelle de la signature est intégrée dans l'article 1322 du Code civil relatif uniquement aux actes sous seing privé. Enfin, cette interprétation est confirmée par les mots "pour l'application du présent article", qui semblent d'ailleurs restreindre considérablement la portée de cette définition. Il en résulte que tant que le législateur belge n'aura pas modifié clairement les règles relatives à l'acte authentique, comme l'a fait le législateur français, celui-ci ne pourra pas être électronique (cf. *infra*, chapitre III).

4. La notion d'écrit

Si la notion de signature englobe désormais les signatures électroniques, on devrait pouvoir en déduire que les écrits électroniques sont, eux aussi, admis au titre de preuve littérale. Toutefois, la question est loin d'être réglée en ce qui concerne les fonctions que l'écrit est appelé à remplir. Dans un premier temps, nous tentons d'y voir clair dans les différents concepts qui entourent la notion d'écrit (a). Nous nous penchons ensuite sur l'opportunité et la formulation d'une définition de l'écrit (b).

a) Le domaine de la preuve littérale

On s'accorde généralement à reconnaître que l'expression "preuve littérale" désigne, en principe, toute forme de preuve par écrit. Dans cette optique, il peut s'agir d'écrits signés ou non, d'originaux ou de copies, etc. Toutefois, on vise le plus souvent sous cette appellation les seuls écrits signés, c'est-à-dire principalement les actes authentiques et les actes sous seing privé[140]. Ces écrits sont rédigés et signés *ad probationem,* aux fins de préconstitution, et considérés comme des preuves complètes, en ce sens qu'elles se suffisent à elles-mêmes pour être pleinement efficaces. Ce n'est pas le cas des autres types d'écrit que sont les commencements de preuve par écrit et les copies, qui eux, doivent être complétés par d'autres éléments pour bénéficier d'une force probante.

Au niveau des notions premières, il est fréquent de retrouver les vocables écrit, titre ou acte, qui sont d'ordinaire utilisés indistinctement pour désigner le document papier rédigé *ad probationem*. Dans certains cas, cet amalgame prête d'ailleurs à de fâcheuses confusions. En effet, le terme acte revêt une double signification. Il peut faire référence à l'accord des volontés (le *negotium*) ou à l'écrit rédigé pour faire preuve de l'accord (l'*instrumentum*). Le terme "titre" est synonyme de l'acte pris dans le second sens indiqué : en principe, il est utilisé seulement dans le registre de la preuve. Ceci ne pose pas problème. Cette distinction est généralement bien maîtrisée.

---

[139] Soulignons uniquement que l'exposé des motifs, en sa page 5 (document 0038/006 disponible sur le site de la Chambre des Représentants : http://www.lachambre.be/documents/38/6.pdf), indique, de manière extrêmement maladroite, que "L'authenticité de l'acte juridique est considérée comme un élément majeur, lorsqu'il s'agit d'apporter la preuve des obligations émanant d'un contrat. L'authenticité d'un contrat a pour objectif de démontrer avec certitude l'identité de celui qui s'est lié de façon contractuelle, la portée exacte de l'obligation ainsi que l'intégrité du contenu de celle-ci". En utilisant le terme authenticité, le législateur n'a manifestement pas voulu faire référence à l'acte authentique, mais simplement aux qualités liées à l'acte en général, qu'il soit authentique ou sous seing privé.

[140] Auxquels il faut assimiler les lettres missives signées (R. MOUGENOT, *La preuve*, tiré à part du "Répertoire Notarial", Bruxelles, Larcier, 2e éd., 1997, p. 127, n° 79) et, demain, les courriers électroniques pourvus d'une signature électronique.

Il convient toutefois de rappeler qu'un écrit peut être exigé tantôt *ad solemnitatem*, et conditionne alors la validité du *negotium*, tantôt seulement *ad probationem*. Dans le premier cas, "la règle de preuve est, en quelque sorte, absorbée par la règle de forme"[141]. Cette remarque est capitale à l'heure où l'on entend élargir la preuve littérale aux écrits sous forme électronique. Les hypothèses où le législateur exige un écrit (papier ?) en dehors de toute préoccupation proprement probatoire sont légion. Par conséquent, une réflexion d'ensemble sur le formalisme légal s'avère nécessaire sous peine de compromettre, quant à sa portée pratique, la réforme envisagée du droit de la preuve. Une telle réflexion est d'ailleurs menée, dans le cadre de la transposition en droit belge de l'article 9 de la directive sur le commerce électronique[142] (cf. *infra*).

Quant à l'écrit, on constate qu'il est fréquemment confondu à l'acte sous seing privé. On lui attribue fréquemment trois qualités fonctionnelles : stabilité, lisibilité, intégrité. Or, si ces qualités le rendent apte à servir au plan probatoire, elles n'appartiennent nullement à l'essence de la notion. En réalité, certaines d'entre elles sont inhérentes, non à l'écrit, mais au papier, qui était le support traditionnel de l'écrit.

Or, dans le contexte électronique, il est parfaitement concevable de maintenir l'inaltérabilité du contenu d'un message alors même que celui-ci change de support[143]. On constate que l'inaltérabilité du contenu du message n'est plus assurée par le support mais par un mécanisme technique (de signature numérique ou autre) qui fige logiquement, et non plus physiquement, le contenu de l'écrit électronique. On constate donc un glissement des garanties, traditionnellement assurées par le papier, vers le mécanisme de signature électronique. Ainsi, il convient d'être attentif à ne pas faire peser sur la notion d'écrit des garanties qui, d'une part, ne relèvent pas de l'écrit, mais du support-papier, d'autre part, ne sont plus assurées dans l'environnement électronique par le support, mais par le mécanisme de signature.

La confusion sur la notion d'écrit est alimentée par bon nombre de législations qui exigent un écrit, notamment à des fins probatoires, sans préciser s'il s'agit d'un simple écrit ou d'un écrit signé. Or, en général, l'écrit doit toujours présenter l'une ou l'autre qualité additionnelle (il doit se trouver sur un support durable, il doit être signé…) pour qu'une force probante particulière lui soit attachée. Ces qualités ne relèvent donc pas de l'essence de l'écrit, mais elles sont requises à titre complémentaire pour qu'il puisse valoir comme preuve. A ce titre, il convient de laisser le soin au juge d'analyser si les garanties supplémentaires, non directement spécifiées par la loi, sont assurées ou non.

La juste attribution des fonctions remplies respectivement par le papier, l'écrit, voire la signature, constitue l'un des points névralgiques de toute réflexion sur l'adaptation du droit de la preuve aux nouvelles technologies. Ce débat est loin d'être anodin au moment où l'on cherche à penser l'équivalence entre l'écriture sur papier et l'écriture électronique[144].

---

[141] R. MOUGENOT, *op. cit.*, p. 128, n° 81.

[142] Voy. en particulier D. GOBERT et E. MONTERO, "Le traitement des obstacles formels aux contrats en ligne", *op. cit.*, pp. 199 à 244.

[143] Tel est le cas, par exemple, d'un fichier signé numériquement qui se trouve sur une disquette, qui est ensuite transféré sur un disque dur et enfin sur un réseau.

[144] Pour ce débat et les solutions proposées, nous renvoyons le lecteur aux contributions suivantes : D. MOUGENOT, " Faut-il insérer une définition de l'écrit dans le Code civil ? ", in *Revue Ubiquité*, 2000/7, pp. 121-128 ; D. GOBERT et E. MONTERO, *J.T.*, *op. cit.*, pp. 121-128 ; P. LECOCQ et B VANBRABANT, *op.cit.*, p. 130-131.

b) Vers une définition légale de l'écrit

Dans un premier temps, face aux adaptations du droit de la preuve aux technologies nouvelles, le législateur belge n'a pas jugé utile de définir le concept d'écrit. L'exposé des motifs de la loi du 20 octobre 2001 précise, en effet, que "Afin d'éviter de devoir introduire dans le Code civil un concept totalement nouveau tel que celui de *document* ou *d'information*, ce qui mettrait en péril la cohérence du Code, le projet ne touche pas au concept *d'écrit"*. Ce même exposé ajoute que "Cette notion n'a nulle part été définie expressément dans le Code civil, mais la jurisprudence et la doctrine s'accordent de plus en plus pour considérer qu'il convient de l'interpréter de façon large et qu'il ne faut pas considérer comme écrit le seul texte manuscrit ou imprimé sur un support papier"[145]. Le législateur belge a ainsi joué la carte de la prudence en estimant que donner une définition de la preuve littérale ou par écrit constitue un exercice délicat qui pourrait susciter plus de difficultés qu'il n'en résout.

Si la loi du 20 octobre 2000 ne donne pas de définition formelle de l'écrit, il n'empêche que l'exposé des motifs aborde la manière dont il faut interpréter cette notion, et cela en deux temps. Dans un premier temps, le texte précise qu'il ne faut plus envisager l'écrit en fonction de son support : l'écrit ne se résume plus nécessairement à un texte rédigé sur support papier. "Même si la discussion s'est souvent focalisée sur la forme du support, il convient de l'élargir [la notion d'écrit] également à la nature de l'information". Dans un deuxième temps, et de manière plus contestable, l'exposé précise les trois qualités fonctionnelles qui caractérisent le document papier (inaltérabilité, lisibilité et stabilité) et en conclut que "dès lors qu'un document électronique présente ces trois caractéristiques, il doit se voir accorder le statut d'écrit au sens du Code civil". Cette vision des choses est surprenante et, en agissant de la sorte, la loi belge fait entrer par la petite porte de l'exposé des motifs un risque de confusion qu'elle a prétendu conjurer en s'abstenant de définir la notion d'écrit dans un article du Code civil. En effet, l'analyse de ces trois fonctions montre que l'exposé des motifs confond le concept d'écrit avec celui d'acte et semble faire peser sur l'écrit des fonctions qui relèvent classiquement de l'écrit signé et du support papier[146].

Confrontés aux incertitudes qui subsistent encore autour de la notion, on constate qu'on ne pourra probablement pas se passer indéfiniment d'une définition légale de l'écrit. Par ailleurs, la réflexion menée dans le cadre de la transposition de l'article 9 de la directive sur le commerce électronique pousse à agir dans ce sens[147].

Pour rappel, l'article 9 de la directive fait obligation aux Etats membres de faire en sorte que "leur système juridique rende possible la conclusion des contrats par voie électronique". A ce titre, ils doivent notamment veiller "à ce que le régime juridique applicable au processus

---

[145] En ce sens, M. FONTAINE, "La preuve des actes juridiques et les techniques nouvelles", in *La Preuve*, colloque U.C.L., 1987, p. 18. ; M. ANTOINE et D. GOBERT, "Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification", *R.G.D.C.*, 1998, n° 4/5, p. 291 ; A. PRÜM, "L'acte sous seing privé électronique : réflexions sur une démarche de reconnaissance", in *Mélanges Michel Cabrillac*, Paris, Litec, 1999, p. 267 ; D. MOUGENOT, "Faut-il insérer une définition de l'écrit dans le Code civil ?", in *Revue Ubiquité*, 2000/7, pp. 121-128. Pour une étude récente et approfondie sur le concept d'écrit au regard des nouvelles technologies, on consultera utilement : D. GOBERT et E. MONTERO, "L'ouverture de la preuve littérale aux écrits sous forme électronique", *J.T.*, n° 6000, pp. 117 à 119.

[146] Pour une analyse critique de cette problématique, le lecteur consultera utilement : D. MOUGENOT, "Faut-il insérer une définition de l'écrit dans le Code civil ?", *op. cit.*, pp. 121-128 ; D. GOBERT et E. MONTERO, *J.T.*, *op. cit.*, pp. 121-128.

[147] Voy. D. GOBERT et E. MONTERO, "Le traitement des obstacles formels aux contrats en ligne", Cahiers du CRID, n°19, *op. cit.*, pp. 199 à 244.

contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ni ne conduise à priver d'effet et de validité juridiques de tels contrats pour le motif qu'ils sont passés par voie électronique". Cette disposition demande donc aux Etats membres d'adapter leur système juridique afin de rendre effectivement possible le recours aux contrats par voie électronique.

Dans le cadre d'une étude concernant la transposition de la directive sur le commerce électronique en droit belge, l'approche suivante a été proposée afin de respecter les exigences de l'article 9[148]. Il s'agit notamment d'adopter un certain nombre de dispositions à caractère transversal, visant à couvrir l'ensemble des textes législatifs et réglementaires posant des exigences formelles susceptibles constituer un obstacle à la conclusion de contrats par voie électronique.

Une première disposition transversale à caractère général est envisagée afin de saisir la notion de formalité au sens large, sans opérer de distinction entre les multiples espèces des formalités. Elle est formulée de la sorte : *"Lorsqu'il est exigé, au cours du processus contractuel, une formalité qui peut faire obstacle, directement ou indirectement, à la conclusion de contrats par voie électronique, celle-ci s'interprète indépendamment de sa forme et de son support. En toute hypothèse, les qualités fonctionnelles de la formalité considérée doivent être préservées"*[149].

D'autres dispositions transversales sont envisagées, s'attachant à certaines formalités dites "classiques" : exigence d'un écrit, d'une signature, de mentions manuscrites… Ainsi, la disposition suivante pourrait être retenue afin de s'attacher à la formalité de l'écrit : *"Lorsqu'une disposition législative et réglementaire exige un écrit au cours du processus contractuel, cet écrit peut résulter d'une suite de lettres, de chiffres ou de tous autres signes intelligibles, accessible pour une consultation ultérieure, quels que soient son support et ses modalités de transmission"*[150].

Une telle approche permet d'évacuer tout interprétation formaliste de la notion. Ainsi, lorsque l'écrit doit présenter des garanties supplémentaires (être signé, être sur un support durable…), il appartiendrait au juge d'apprécier souverainement, au cas par cas, le respect de ces exigences, sachant que ces dernières doivent être interprétées largement, en vertu de la disposition transversale à caractère général, afin de pouvoir prendre la forme électronique, sans toutefois porter préjudice au niveau de protection assuré par la formalité.

On note que les qualités ici requises sont indéniablement la lisibilité et la stabilité, puisqu'une consultation ultérieure doit être possible. Par contre, on ne trouve pas l'exigence d'intégrité, celle-ci étant le propre de l'écrit *signé*, non de l'écrit. Or, comme on le sait, c'est la signature qui remplit la fonction d'intégrité dans l'environnement numérique.

Un mot d'explication doit encore être donné de la notion de "processus contractuel", notion nouvelle dans notre droit. Ces termes ont une portée très large. En effet, ils ne se limitent pas à l'étape de conclusion du contrat, mais comprennent toutes les étapes allant de la période précontractuelle (prospectus publicitaire, offre…) jusqu'à l'archivage, en passant par les

[148] *Idem*, pp. 240 et s., n^{os} 441 et s.
[149] Voy. l'art. 17, § 1er, du texte législatif proposé en annexe de l'ouvrage *Le commerce électronique européen sur les rails ?…*, *op. cit.*, p. 417.
[150] Voy. l'art. 17, § 2, al. 1er, *idem*, p. 418.

modalités relatives à l'exécution du contrat (facturation, paiement, livraison) ou à la fin de celui-ci (terme, résiliation), à sa modification, à son enregistrement, etc.[151]

5. La distinction original/copie dans l'environnement numérique

Nulle part, les notions d'original et de copie ne sont définies par le législateur belge. Aussi, afin d'apprécier la portée exacte de cette distinction dans un contexte numérique, convient-il d'abord de préciser les contours de ces concepts, en doctrine et en jurisprudence (a), avant de se pencher sur la valeur probante des copies (b).

a) Précisions sur les notions d'original et de copie

"La notion d'original désigne tout acte – authentique ou sous seing privé – pourvu qu'il soit signé"[152]. C'est dans la seule signature que réside la distinction entre copie et original, la première n'étant qu'une transcription non signée du second[153]. C'est donc sur base de ce seul critère qu'il convient d'attribuer à un écrit la qualité d'original ou de copie.

Dès lors, on ne s'attachera pas au caractère unique de l'écrit pour lui conférer le statut d'original[154], ni au fait qu'il demeure sur son support d'origine (la nature de ce support étant, par ailleurs, indifférente). En outre, le fait que l'intégrité de l'écrit soit préservée ne suffit pas à en faire un original, dès lors que cet écrit n'est pas signé[155].

Auparavant, les techniques existantes de reproduction d'un original ne pouvaient conduire qu'à des copies, au sens juridique du terme, à défaut de signature apposée directement sur la reproduction de cet écrit. Il en va ainsi d'une photocopie, d'une télécopie, d'un microfilm ou de l'usage du papier carbone. Bien entendu, l'apposition ultérieure d'une signature sur une copie lui confère aussitôt la qualité d'original.

L'avènement de l'informatique est venue semer le trouble dans la distinction établie entre copie et original. Dans les premiers temps, toute reproduction de données informatiques fut analysée en copie. Aujourd'hui, le recours à une signature numérique basée sur un système de cryptographie asymétrique oblige à revoir cette analyse. Désormais, il est possible de reproduire un écrit numérique en copie ou en original. En effet, la transmission ou la reproduction d'un fichier digitalement signé n'affecte pas le lien (logique) qui unit la signature au document signé. A défaut d'une telle signature, on a affaire à une copie[156].

Ainsi, un original sur papier peut être scanné, mais l'image numérique qui en résulte n'en sera qu'une copie. Il en ira de même, *a fortiori*, si cette image numérique est par la suite imprimée sur papier. Par contre, si le fichier contenant l'image ainsi numérisée est digitalement signé (par le même auteur que celui de l'original sur papier), on obtiendra un original.

---

[151] D. GOBERT et E. MONTERO, "Le traitement des obstacles formels aux contrats en ligne", *op. cit.*, n^os^ 380 et 443.
[152] D. GOBERT et E. MONTERO, "L'ouverture de la preuve littérale aux écrits sous forme électronique", *op. cit.*, p. 122.
[153] H. DE PAGE, *Traité*, t. III, 3^e^ éd., n° 832 ; R. MOUGENOT, *op. cit.*, p. 185, n° 187 ; N. VERHEYDEN-JEANMART, *Droit de la preuve*, Bruxelles, Larcier, 1991, p. 201, n° 417.
[154] Voy., à cet égard, la formalité des originaux multiples prescrite par l'article 1325 du Code civil.
[155] D. GOBERT et E. MONTERO, "L'ouverture de la preuve littérale aux écrits sous forme électronique", *op. cit.*, pp. 127-128.
[156] A ce sujet, voy. aussi E. DAVIO, " Preuve et certification sur Internet ", *op. cit.*, p. 664.

b) La valeur probante des copies

Selon l'article 1334 du Code civil, *" Les copies, lorsque le titre original subsiste, ne font foi que de ce qui est contenu au titre, dont la représentation peut toujours être exigée "*. Ce statut inférieur de la copie par rapport à l'original s'explique par l'absence de signature, mais aussi par les risques de manipulation du contenu que comporte l'opération de reproduction.

Dans un environnement numérique, il est aisé de créer un document qui se veut la copie d'un acte original, et qui est, plus exactement, un simple écrit non signé, dont l'original ne peut être produit. Dans ce cas, même le régime strict de l'article 1334 ne pourra s'appliquer au message reçu, qui ne peut être regardé comme une 'copie' au sens de cette disposition. Tout au plus, pareil message de données pourra-t-il être reçu comme commencement de preuve par écrit (art. 1347) ou, plus vraisemblablement, comme simple présomption.

Toutefois, certains auteurs considèrent que la règle de l'article 1334 pourrait être appelée à jouer un rôle important dans l'avenir, avec l'informatisation de la Justice : "A court terme, en attendant que les écrits signés numériquement puissent être envoyés directement, par voie électronique, aux greffes (informatisées) des tribunaux, ces écrits seront vraisemblablement produits en copie papier. Dans cette hypothèse, le titre original pourra, sur demande, être représenté en justice, conformément au prescrit de l'article 1334. A moyen terme, il se peut aussi que, pour des raisons de commodité, des copies papier soient plus volontiers utilisées dans l'administration de la justice, alors même que les écrits signés, tenant lieux d'originaux, pourraient être produits sous forme de fichiers informatiques ou expédiés aux greffes électroniques"[157].

B. La durée de conservation et les délais de prescription

Lorsqu'on envisage la conservation d'un document à des fins probatoires, on constate que la durée de cette conservation est étroitement liée aux délais de prescription des droits et obligations afférents au dit document[158]. En effet, qui entend se prémunir d'une éventuelle contestation sera bien avisé de conserver les preuves de l'existence de son droit ou de l'exécution de ses obligations durant toute la durée du délai de prescription, pendant lequel une action est susceptible d'être intentée par ou contre lui.

Après un bref rappel des principales règles de prescription (1), on examine l'impact de ces règles sur la conservation de documents sous une forme électronique (2).

1. Rappel des règles principales en matière de prescription

Notre propos n'est pas ici de pénétrer les arcanes du droit de la prescription, ni d'énumérer à l'infini la liste des différents délais existants, d'autant qu'il nous faudrait pour cela envisager les prescription en droit civil, en droit du travail, en droit des assurances, en droit fiscal, etc. Simplement, afin de mieux saisir la diversité des délais pendant lesquels il convient de conserver des moyens de preuve, nous nous en tiendrons à quelques hypothèses (a) et règles générales (b).

[157] D. GOBERT et E. MONTERO, "L'ouverture de la preuve littérale aux écrits sous forme électronique", *op. cit.*, p. 128.

[158] E. CAPRIOLI, " Variations sur le thème du droit de l'archivage dans le commerce électronique ", *Petites affiches*, 18 août 1999, p. 8.

a) La durée du délai de prescription

Notre droit connaît de multiples délais de prescription, disséminées notamment dans les articles 2262 et suivants du Code civil, mais aussi dans de nombreuses législations particulières. A titre d'illustration, citons :

- la prescription trentenaire
  - pour les actions réelles (art. 2262 C. civ.) ;
  - pour la tierce opposition (art. 1128 C. jud.) ;
- la prescription décennale :
  - pour les actions personnelles (art. 2263, al. 1er, C. civ.), à l'exception des actions en réparation d'un dommage fondées sur une responsabilité extra-contractuelle ;
- la prescription quinquennale :
  - pour les actions en réparation d'un dommage fondées sur une responsabilité extra-contractuelle, à partir du jour de la connaissance du dommage, avec un maximum de 20 ans à partir du fait dommageable (art. 2263, al. 2 et 3, C. civ.) ;
  - pour les arrérages de rentes perpétuelles et viagères, ceux des pensions alimentaires, les loyers des maisons, les intérêts des sommes prêtées, et généralement tout ce qui est payable par années, ou à des termes périodiques plus courts (art. 2277 C. civ.) ;
- la prescription triennale :
  - pour toute action dérivant d'une police d'assurance (art. 32 de la loi du 11 juin 1874 contenant les titres X et XI, livre Ier, du code de commerce. Des assurances en général - De quelques assurances terrestres en particulier) ;
  - pour toutes les actions résultant de la lettre de change contre l'accepteur (art. 70 C. com) ;
- la prescription de six mois :
  - en ce qui concerne le chèque, pour les actions en recours du porteur contre les endosseurs, le tireur et leurs autres obligés (art. 52 de la loi du 1er mars 1961 concernant l'introduction dans la législation nationale de la loi uniforme sur le chèque et sa mise en vigueur).

En ce qui concerne précisément les juges, huissiers, avocats et experts, l'action en responsabilité en cas de perte ou de destruction des documents qu'ils ont l'obligation de conserver est soumise à des prescriptions abrégées. Dès lors, la durée minimale de conservation des pièces correspond à cette prescription abrégée.

Juges :		5 ans après le jugement des procès
Huissiers de justice :		2 ans après l'exécution de la commission ou la signification des actes
Avocats :		5 ans après la fin de la mission
Experts :		10 ans après la fin de la mission
	ou	5 ans après le dépôt de leur rapport

b) L'interruption et la suspension de la prescription

Il convient en outre de tenir compte d'une éventuelle interruption ou suspension de la prescription.

En effet, lorsqu'il y a interruption de la prescription, un nouveau délai de prescription prend cours, et il n'est plus tenu compte du temps déjà écoulé. Les principales causes d'interruption

de la prescription sont : une citation en justice, un commandement ou une saisie, signifiés à celui qu'on veut empêcher de prescrire (art. 2244 C. civ.) ; ou la reconnaissance par le débiteur du droit de celui contre lequel il prescrivait (art. 2248 C. civ.).

La suspension de la prescription signifie qu'on n'en tient pas compte pendant un certain temps, ce qui a pour effet de prolonger la durée de la prescription du temps pendant lequel elle est restée en suspens[159]. Le temps écoulé avant la suspension n'est pas perdu : " le bénéficiaire de la prescription pourra l'ajouter à celui qui s'écoulera depuis le moment où la cause de suspension aura disparu "[160]. Ainsi, par exemple, la prescription est suspendue entre époux pendant toute la durée du mariage (art. 2253 C. civ.), elle ne court pas non plus contre les mineurs et les interdits, sauf en ce qui concerne les courtes prescriptions des articles 2271 à 2277 du Code civil et les autres cas déterminés par la loi (art. 2252 C. civ.)[161].

2. Implications pratiques de la prescription au niveau de la conservation de documents

En pratique, pour la conservation de documents afférents à des droits ou obligations, il faudra tout d'abord tenir compte du point de départ du délai. Il convient à cet égard de souligner que la prescription pourrait commencer à courir postérieurement à la création et à l'archivage du document.

Ensuite, en fonction des droits ou obligations auxquels le document se rapporte, il faut envisager le délai de prescription prévu. Notons qu'il n'est pas à exclure que pour un même document, plusieurs droits ou obligations soient en jeu, avec des prescriptions différentes quant à leur durée ou quant au point de départ du délai.

Enfin, le cours de la prescription pourrait se trouver interrompu ou suspendu. Dans le premier cas, un nouveau délai de prescription prend cours ; dans le second, le délai est prolongé du temps pendant lequel la prescription est restée en suspens. Quoi qu'il en soit, il conviendra alors de conserver le document plus longtemps que prévu.

Dès lors, la durée de conservation d'un document en fonction des règles de prescription pourra s'étendre de quelques mois à plus de trente ans.

---

[159] M. REGOUT-MASSON, " La prescription en droit civil ", *op. cit.*, p. 51.
[160] H. DE PAGE, t. VII, n° 85, p. 73.
[161] Pour davantage de développements sur les causes de suspension et d'interruption de la prescription en droit civil, en droit du travail, en droit des assurances et en droit pénal, nous renvoyons à l'ouvrage collectif suivant : *La prescription*, Liège, Formation permanent CUP, 1998.

II. L'OBLIGATION LÉGALE DE CONSERVATION

De nombreux textes légaux imposent une obligation de conservation de documents, dans de nombreuses matières : droit fiscal, droit comptable, droit social, droit médical, droit civil, droit judiciaire...

Dans le cadre du projet e-Justice, nous concentrons notre étude sur les obligations légales de conservation touchant, de près ou de loin, les acteurs du monde judiciaire : les greffiers (A), les juges, les huissiers, les avocats et les experts (B), ainsi que les notaires (C). Par ailleurs, on ne saurait aborder la question de la conservation de documents sans parler des Archives du Royaume (D). Enfin, un mot sera dit des registres officiels (E).

A. Le Code judiciaire

En vertu de l'article 173, al. 1er, du Code judiciaire, le greffier est chargé de la conservation des archives de la juridiction près laquelle il est établi :
- il garde les minutes des actes qu'il est chargé de passer, les registres et tous les actes afférents à cette juridiction,
- il conserve la documentation législative, jurisprudentielle et doctrinale à l'usage des juges,
- il tient les registres et les répertoires (voy. notamment les art. 174[162], 1027, 1047, 1185, 1311 et 1341 C. jud.),
- il assure la conservation des valeurs, documents et objets déposés au greffe en vertu de la loi.

Il revient au Roi de déterminer les modalités d'application de l'article 173. Toutefois, à ce jour, aucun arrêté royal d'exécution n'a été adopté. Sans doute, dans le cadre de l'informatisation de la Justice, un arrêté royal pourrait établir les modalités techniques et les conditions de conservation de documents électroniques au greffe.

Le greffier assure également la conservation des choses saisies en matière répressive et déposées à son greffe (art. 1er de l'AR n° 260 du 24 mars 1936 sur la détention au greffe et la procédure en restitution des choses saisies en matière répressive, *M.B.*, 26 mars 1936).

Il tient en outre le rôle général des affaires ainsi que les rôles particuliers (art. 711 et s. C. jud.).

Le greffier est également chargé de la constitution et de la garde des dossiers de la procédure (art. 720 et s. C. jud.). Or, la conservation de ces documents est vouée à s'étendre sur une longue période, étant donné que le délai pour faire tierce opposition contre un jugement est de trente ans (art. 1128 C. jud.).

Notons encore que le greffier en chef répond des objets dont il assure la conservation ou la garde et est responsable, à l'égard des parties, des pièces produites (art. 175 C. jud.).

De prime abord, aucun des articles précités ne semble empêcher la conservation de ces documents sous forme électronique. Les termes "minutes", "actes", "registres", "répertoires", "dossiers", "rôle", "pièces" ne font référence à aucune forme et à aucun support en particulier.

[162] Mis en exécution par l'arrêté royal du 6 février 1970 relatif à la tenue par le greffier d'un répertoire des actes du juge et d'un répertoire des actes du greffe, *M.B.*, 21 mars 1970.

Néanmoins, ils impliquent de toute évidence le recours à l'écrit. C'est donc la notion même d'écrit en droit judiciaire qui doit être examinée pour voir quelles sont les qualités qu'on y attache, et si les documents sous forme électronique revêtent ces qualités. A l'heure actuelle, la définition de la notion d'écrit n'est à l'étude qu'en ce qui concerne le "processus contractuel" (*supra*, point I.A.4). L'exigence d'un écrit au cours de la procédure judiciaire n'entre donc pas dans ce champ d'application. Il conviendra dès lors de s'interroger sur l'opportunité d'une définition de l'écrit en droit judiciaire.

Par ailleurs, d'autres dispositions du Code judiciaire relatives à ces documents ont manifestement été formulées dans un contexte papier :

- art. 713 : "le rôle général est *coté par première et par dernière et paraphé sur chaque feuille* (...)"
- art. 720 : "Le greffier inscrit *sur la chemise du dossier* la date de la mise au rôle et le numéro d'ordre de la cause"
- art. 723, § 3 : "Le greffier fait mention du recours *en marge* de la décision"
- art. 1027 : "Le requérant reproduit *au pied de la requête* [unilatérale] l'inventaire des pièces numérotées et *enliassées* qu'il joint à celle-ci"
- art. 1099 C. jud. : "Le greffier constate la remise des requêtes et mémoires au moyen de *notes marginales*, qu'il signe en indiquant la date de réception.
  Il *cote et paraphe les pièces jointes*, constate leur nombre par une *note signée en marge de l'inventaire* et délivre récépissé au déposant, s'il en est requis."
- art. 1er de l'AR du 6 février 1970 relatif à la tenue par le greffier d'un répertoire des actes du juge et d'un répertoire des actes du greffe : "Les greffiers y inscrivent jour par jour, *sans blanc ni interligne*, la date des actes et leur nature. Les répertoires sont *paginés* (...)"

Il conviendra dès lors d'adapter ces exigences formelles au contexte numérique. Dans cette démarche, il faudra sans conteste adopter l'approche fonctionnelle et s'attacher davantage à la fonction de ces formalités qu'à leur stricte transposition dans des formes numériques. Ainsi, lorsqu'on exige une inscription "sans blanc ni interligne", c'est en réalité l'intégrité de l'acte qu'on veut préserver, en évitant toute insertion ultérieure et toute modification de l'ordre des inscriptions. Or, dans l'environnement numérique, une inscription sans blanc ni interligne dans un document électronique ne permettra certainement pas d'en protéger le contenu ! Le même raisonnement peut être tenu pour l'exigence de pagination des répertoires. Dès, lors, on sera attentif à recourir à un autre moyen pour assurer l'intégrité de l'acte.

Notons encore que les exigences d'inscription peuvent être interprétées largement, au-delà de la seule inscription manuscrite, toujours dans une approche fonctionnelle. Une modification des textes ne nous paraît pas nécessaire à ce niveau.

Signalons enfin, à propos des archives judiciaires, qu'une convention est actuellement en préparation entre le Ministère de la Justice et les Archives du Royaume afin de fixer un tableau de tri des documents, à destination des greffes des cours et tribunaux, mais aussi des parquets. Il s'agit de déterminer avec précision, pour chaque juridiction, quels sont les documents qui doivent être conservés et quelle doit être la durée de cette conservation avant d'être éliminés ou versés aux Archives du Royaume, et ce, quelles que soient la forme et la structure de ces documents.

B. Les articles 2276 et suivants du Code civil

Par ailleurs, on relève dans les articles 2276 et suivants du Code civil, relatifs à la prescription, une obligation indirecte de conservation de documents à charge de certaines professions, telles que les juges, les huissiers de justice, les avocats ou les experts. En effet, après un certain délai, les membres de ces professions se voient déchargés de toute responsabilité en cas de perte ou de destruction de pièces qui leur ont été confiées, lorsqu'un dommage en résulte[163]. Implicitement, il s'agit là d'une obligation de conservation pesant sur ces professions pendant toute la durée du délai, sous peine de voir leur responsabilité engagée. Le terme "pièces" ne pose pas de problème particulier au regard des NTIC. Il nous paraît suffisamment large pour englober également les documents électroniques dont ces personnes auraient la garde, aucune référence n'étant faite à la forme ou au support de ces pièces.

Les juges sont déchargés des pièces cinq ans après le jugement des procès à l'occasion desquels elles leur furent confiées, en vertu de l'article 2276 du Code civil. Cette courte prescription s'explique par le fait que lorsque le procès est terminé, les juges n'ont plus besoin de ces pièces. "Il est donc probable qu'ils les rendent aux parties ou que celles-ci les réclament si les pièces peuvent encore être utiles. Si les pièces deviennent inutiles, il y avait une raison de plus de limiter la responsabilité pour la restitution des papiers sans valeur"[164].

Les huissiers de justice sont déchargés des pièces deux ans après l'exécution de la commission ou de la signification, en vertu de l'article 2276, alinéa 2, du Code civil. Certains ont justifié ce bref délai par le fait que le ministère des huissiers comporte plus de rapidité[165], mais LAURENT n'est pas de cet avis, ne voyant, en fin de compte, aucune bonne raison à cette différence de durée de la prescription[166].

L'article 2276*bis* du Code civil décharge l'avocat de la conservation des pièces cinq ans après l'achèvement de sa mission, sauf lorsqu'il a été expressément constitué dépositaire de pièces déterminées. Cet article a été introduit par la loi du 8 août 1985 relative à la prescription en matière de responsabilité professionnelle de l'avocat et de conservation des archives (*M.B.*, 14 sept. 1985). Auparavant, les avocats devaient conserver ces archives pendant trente ans, au risque d'actions en responsabilité professionnelle éventuelles. Cette situation n'était pas sans poser de sérieux problèmes matériels aux avocats et aux ayant-droits des avocats décédés. C'est la raison pour laquelle le législateur a permis aux avocats de se décharger de leurs archives après un délai inférieur à trente ans, fixé à cinq ans afin d'aligner le sort des avocats sur celui des juges[167].

L'article 2276*ter* du Code civil décharge les experts de la conservation des pièces dix ans après l'achèvement de leur mission ou, si celle-ci leur a été confiée en vertu de la loi, cinq ans après le dépôt de leur rapport. Il semble que la notion d'expert doive s'entendre de manière extrêmement large, étant donné les exemples fournis par les travaux préparatoires de la loi du 19 février 1990 insérant dans le Code civil un article 2276*ter* relatif à la prescription de la responsabilité des experts et de leur action en paiement de leurs frais et honoraires (*M.B.*, 30 mai 1990) : experts médecins, experts architectes et ingénieurs, experts comptables et fiscaux, experts de l'administration, experts immobiliers pour les expertises préalables en matière de

[163] Voy. F. POILVACHE, " L'article 2276*ter* nouveau du Code civil soumettant la responsabilité des experts et leurs créances d'honoraires à des prescriptions abrégées ", *J.T.*, 1991, p. 293 ; D. STERCKX, " Premiers commentaires sur l'article 2276*bis* du Code civil ", *J.T.*, 1985, p. 535.
[164] LAURENT, *Principes de droit civil*, t. XXXII, n° 481.
[165] TROPLONG, *De la prescription*, n° 999.
[166] LAURENT, t. XXXII, n° 485.
[167] M. REGOUT-MASSON, " La prescription en droit civil ", in *La prescription*, Liège, Formation permanente CUP, 1998, p. 47.

droit de succession, arbitres en matière de fixation des revenus cadastraux…[168] En bref, l'article 2276*ter* est d'application chaque fois " qu'une mission [est] confiée à un spécialiste par une ou plusieurs personnes privées ou publiques ou par le juge et qu'elle [a] pour objet de donner un avis sur des questions de fait, techniques ou scientifiques "[169].

C. La loi du 25 ventôse – 5 germinal an XI contenant organisation du notariat

La conservation de documents fait partie inhérente de la fonction notariale (voy. les art. 1er, 20, 22, 29 et 62 de la loi). A cet égard, on sait que cette conservation peut s'étendre sur une très longue durée. En effet, l'article 62 ne prévoit la possibilité de les transmettre aux Archives du Royaume qu'après 50 ans. Cette possibilité se mue en obligation après 75 ans.

Les termes employés par les articles précités ne font référence à aucune forme ni à aucun support particulier pour la conservation des actes, contrats, minutes, répertoires, tables, etc. Il est évident que tous ces documents impliquent eux aussi le recours à l'écrit, ce qui nous ramène à la réflexion menée ci-dessus. Il conviendra également d'examiner les autres dispositions de la loi, afin de voir si leur formulation n'a pas été envisagée dans le seul contexte du papier.

Concernant les problèmes spécifiques posés par la conservation de documents par les notaires, nous renvoyons à la partie consacrée à l'acte authentique électronique.

D. La loi du 24 juin 1955 relative aux archives

On n'oubliera pas de citer le rôle capital des Archives du Royaume, chargées de la responsabilité et de la gestion du patrimoine archivistique belge. Les tâches des Archives du Royaume sont précisées par la loi du 24 juin 1955 relative aux archives (*M.B.*, 12 août 1955)[170], dont l'article 1er dispose :

"Les documents datant de plus de cent ans conservés par les tribunaux de l'ordre judiciaire, le Conseil d'État, les administrations de l'État et les provinces sont déposés – sauf dispense régulièrement accordée – aux archives de l'État.

Les documents datant de plus de cent ans conservés par les communes et par les établissement publics peuvent être déposés aux archives de l'État. (…)

Il pourra être procédé au dépôt aux archives de l'État des documents ayant moins de cent ans et ne présentant plus d'utilité administrative, à la demande des autorités publiques auxquelles elles appartiennent.

Les archives appartenant à des particuliers ou des associations privées peuvent également être transférées aux archives de l'État, à la demande des intéressés".

La loi emploie les termes "documents" et "archives", très généraux. Il n'est fait aucune référence à la forme et au support de ces documents et archives. Dès lors, la loi sur les

[168] *Doc. parl.*, Ch. repr., sess. extr., 1988, n° 367/1, p. 1.
[169] F. POILVACHE, " L'article 2276*ter* nouveau du Code civil… ", *op. cit.*, pp. 292-293.
[170] Voy. également l'arrêté royal du 12 décembre 1957 pris en exécution de la loi sur les archives, *M.B.*, 12 déc. 1957.

archives ne pose aucun obstacle à la conservation de documents électroniques par les Archives du Royaume.

Toutefois, si une modification de la loi sur les archives n'est pas nécessaire, il convient d'envisager l'adoption d'une réglementation fixant les conditions de conservation des documents sous forme électronique. Nous reviendrons ultérieurement sur ces conditions et sur le rôle que les Archives du Royaume pourraient éventuellement jouer en matière de régulation ou de conseil dans la conservation des documents électroniques dans le secteur public.

E. Remarque : le cas des registres officiels

Ajoutons à cette énumération les innombrables registres officiels : registre de la population, registre électoral, registres d'état civil, conservation des hypothèques, registres fonciers, registre du commerce, registre des détenus, casier judiciaire…

Concernant ces registres, nous soulignons la nécessité d'une étude approfondie et spécifique pour chacun d'eux, en fonction de leurs particularités respectives. A cet égard, des études minutieuses ont été menées ou sont en cours (concernant, notamment, le registre électoral[171] ou le registre d'état civil) dans le cadre du projet DAVID (Digitale Archivering in Vlaamse Instellingen en Diensten), spécifique à l'archivage électronique dans les institutions et les administrations flamandes.

[171]Voy. F. BOUDREZ et S. VAN DEN EYNDE, *Digitale archivering van het kiezersregister*, disponible à l'adresse suivante : http://www.dma.be/david/index2.htm.

III. LES CONDITIONS D'UNE CONSERVATION FIABLE DANS L'ENVIRONNEMENT NUMÉRIQUE

La conservation de documents électroniques devra présenter toutes les garanties de fiabilité, qu'il s'agisse de mener à bien une mission de conservation, dans le cas d'un professionnel, ou de produire un document ayant la force probante d'un acte sous seing privé ou d'un acte authentique.

Dans un cas comme dans l'autre, les conditions *sine qua non* d'une conservation fiable sont la stabilité (A), la lisibilité (B), et l'intégrité (C) du document électronique. Il peut également y avoir, dans certaines hypothèses, une exigence de confidentialité (D).

A. Stabilité et longévité du support

Le support même de l'archive électronique pose problème. La stabilité suppose que le support se dégrade peu, afin de permettre la conservation des informations qu'il contient, en vue d'une consultation ultérieure. Or, une information numérique stockée sur un disque ou une bande ne pourra perdurer et être consultée que si le support qui la stocke demeure en bon état.

Notons que l'exigence de stabilité ne signifie en aucun cas que le document doit demeurer sur le même support tout au long de son existence. Ainsi, il n'est pas exclu qu'il transite par des supports de natures différentes[172]. A titre d'exemple, des conclusions envoyées au greffe par courrier électronique se voient d'abord disséminées sur le réseau par paquets, voyageant par ondes hertziennes ou fibres optiques, aiguillés par une multitude de routeurs vers le serveur SMTP final, à partir duquel il sera finalement téléchargé sur le disque dur de l'ordinateur du greffe, stocké dans un fichier, éventuellement imprimé sur papier, et enfin enregistré sur un autre support pour être archivé. Une fois archivé, le document peut encore changer de support au fil du temps, en fonction des nécessités techniques (conservation du document) ou pratiques (consultation du document).

1. La fragilité des supports numériques

a) Problèmes

La qualité des bandes ou des disques varie selon le matériau utilisé, la production et le contrôle de qualité. De plus, en exploitation, ces supports peuvent s'altérer par un transport fréquent, la maladresse dans la manipulation par les utilisateurs, les impuretés, les variations de températures, l'humidité de l'air, la magnétisation perturbée par un champ magnétique, bref autant de facteurs qui favorisent la dégradation des données numériques.

L'utilisation des données numériques peut aussi conditionner leur conservation. Cela concerne uniquement les supports magnétiques qui ont tendance à présenter des signes de faiblesse s'ils ne sont pas utilisés régulièrement.

Tout comme l'archivage papier, l'archivage électronique pose des problèmes en matière de méthodes de conservation, qui peuvent varier en fonction du support choisi. Un support magnétique, utilisant une tête de lecture électronique, se montre particulièrement sensible aux poussières, mais également, comme déjà évoqué ci-dessus, aux conditions de température et d'humidité du lieu de stockage. Une tête de disque dur actuel, par exemple, flotte à quelques

[172] En ce sens, D. MOUGENOT, " Faut-il insérer une définition de l'écrit dans le Code civil ? ", *op. cit.*, p. 123.

micromètres de la surface du disque magnétique : un cheveu (75 µm –microns -) suffirait à la détruire. Les lecteurs de disquettes et de bandes ont des têtes situées plus haut, pour éviter ce genre de catastrophe, mais cela, au détriment de leur précision, et donc de la densité des informations stockées sur le support. Cependant, le disque magnétique d'une disquette est exposé au monde extérieur, ce qui le rend plus vulnérable.

b) Solutions techniques

La réponse au problème de la conservation est fondamentalement la même que celle apportée aux risques inhérents au stockage de papier, lequel doit également être préservé du feu, de l'humidité, etc. Les supports sensibles de stockage électronique doivent ainsi être confinés dans des armoires ignifugées, maintenues à température et humidité constantes, ce qui présente l'énorme avantage du gain en volume à sécuriser.

A une échelle plus restreinte, une disquette "archivée " pourra par exemple être conditionnée hermétiquement, garantissant une durée de conservation plus grande qu'une disquette posée sur un coin de bureau.

En ce qui concerne le problème de la dégradation des performances d'une bande magnétique non utilisée, une simple re-lecture/ré-écriture régulière des informations permettra une remagnétisation des particules magnétiques composant la surface du support. Ce dernier problème met en évidence un nouvel enjeu pour l'archivage électronique (qui n'existait pas pour l'archivage traditionnel), qui est de trouver un équilibre entre une conservation de qualité (hermétique, …) et une utilisation régulière pour favoriser la remagnétisation.

Pour apporter une réponse au problème de la (relative) fragilité du support, les départements de recherche et développement des fabricants travaillent à la mise au point de nouveaux matériaux, voire de nouvelles techniques, plus résistantes. Ainsi, les performances de stockage s'améliorent en même temps que celles de la durée de vie. Si la bande magnétique permet à l'heure actuelle de stocker de grandes quantités de données[173], l'arrivée des supports optiques a permis d'offrir un support durable et résistant aux agresseurs du support magnétique. Demain, nous aurons ainsi jusqu'à 5,4 Go de données sur un disque DVD-RAM[174] de 12 cm. Il existe également des disques magnéto-optiques (information stockée de manière magnétique, mais sur un support qui doit être altéré par un laser pour changer de polarité), mais ceux-ci sont moins répandus.

La recherche planche à l'heure actuelle sur un nouveau moyen de stockage, basé sur la technique de l'hologramme. Celle-ci devrait permettre de stocker de très importantes quantités de données dans un volume réduit.

2. L'obsolescence du matériel informatique

a) Problème

C'est un lieu commun : le matériel informatique est lui aussi frappé d'obsolescence à un rythme pour le moins rapide, bien que les choses évoluent moins vite dans les grands centres

[173] IBM propose actuellement une solution de stockage offrant jusqu'à 14,4 To de données compressées, voire, pour les grandes entreprises, une solution allant jusqu'à 496,2 To de données compressées, pouvant encore être accrue.
[174] Le DVD-ROM permet, lui, de stocker jusqu'à 18 Go de données

informatiques que pour les produits destinés au grand public. Cependant, l'évolution est inéluctable. Citons à titre d'exemple les disquettes 5"¼ d'il y a moins de 10 ans, ou les disques durs de la même époque inutilisables sur les ordinateurs actuels, malgré leur longue période d'utilisation. De tels cas de rupture de compatibilité ascendante sont malheureusement fréquents.

Il n'est donc pas sage de stocker aujourd'hui toutes ses archives sans penser aux moyens de demain : que ferait-on aujourd'hui de l'information stockée autrefois sur cartes perforées, sans lecteur approprié ? Or de tels lecteurs ont depuis longtemps rang d'antiquité, tant l'évolution des technologies informatiques est rapide.

b) Solutions techniques

Trois solutions sont généralement avancées pour faire face au problème de l'obsolescence des supports[175] :

- La copie " en dur " (*hard copy*) :

Cette solution signifie simplement que pour assurer la préservation à long terme d'un document numérique, on l'imprime sur papier ou on le microfilme. Certes, cette technique présente l'avantage de résoudre le problème de l'obsolescence du support et des logiciels, mais elle nous prive de tous les avantages liés au support numérique : économie d'espace, rapidité d'accès aux données (et donc efficacité), etc. En outre, tous les documents multimédia ne sont pas convertibles sous cette forme (images animées, sons...). Aussi, il nous semble que cette solution devrait être réservée aux seuls cas où il s'avère impossible de conserver de manière fiable un document sous forme électronique.

- La conservation du matériel informatique

On peut également envisager la constitution de " musées de l'informatique ", chargés de conserver le matériel informatique et les logiciels ayant créé le document digital, afin de pouvoir continuer à lire ce dernier sur le support et dans le format d'origine. A supposer qu'une telle solution soit réalisable, on imagine le coût d'une telle opération, l'exptertise nécessaire – la plupart des informaticiens d'aujourd'hui ignorant le langage de programmation des logiciels trop anciens –, et le problème de l'entretien et du remplacement des pièces défectueuses (difficulté de se procurer des pièces de rechange). Aussi convient-il d'écarter cette hypothèse.

- La migration

Afin d'éviter de se retrouver avec des supports illisibles par les machines actuelles, la technique de la migration des données offre une solution au problème soulevé plus haut. Cette technique consiste à recopier des données numériques d'un support devenu obsolète sur un support récent, de manière à faire persister les données électroniques et cela, au fur et à mesure de l'évolution des techniques[176]. Notons que cette migration peut s'établir également au niveau du format de fichier ou du système d'exploitation (cf. *infra*, point B). Une telle

[175] F. BOUDREZ, *Het digitale archiveringssysteem*, Etude menée dans le cadre du projet DAVID, Anvers, juin 2001, disponible en ligne à l'adresse : http://www.dma.be/david/index2.htm.
[176] Pour de plus amples développements concernant cette technique, voy. F. BOUDREZ, *op. cit.*, pp. 8-9.

solution est évidemment coûteuse, étant donné le coût du nouveau support et le temps de recopie non négligeable.

Malgré son caractère onéreux, cette technique de duplication de l'information de support en support offre une méthode de stockage virtuellement illimitée dans le temps, la solution ultime étant, bien entendu, la création d'un support à durée de vie illimitée qui ne nécessiterait donc pas de reproduction.

B. Lisibilité : l'obsolescence des logiciels

Par l'exigence de lisibilité, on entend l'accessibilité à la compréhension humaine des informations contenues dans le document, grâce à un procédé approprié[177]. Alors que cette exigence est directement rencontrée par le support papier, l'information stockée sous format électronique est par essence illisible pour l'homme, qui devient dès lors complètement dépendant des machines aptes à restituer le contenu de ses archives. Se pose alors la question de la pérennité du logiciel de lecture/écriture.

1. Problèmes

Même si les supports sont bien traités, le logiciel ayant servi à générer les données stockées peut poser problème. En effet, la plus parfaite des conservations de matériel ne servirait à rien s'il est devenu impossible de lire les informations stockées sur le support. L'évolution permanente des programmes de traitement de données (lecture, écriture…) et donc leur obsolescence continuelle pose le risque de ne plus pouvoir ouvrir certains fichiers[178].

Toutefois, un support impeccable et une application de lecture compatible aux données numériques concernées ne suffisent pas. Il est en effet nécessaire de disposer du système supportant l'application de lecture : le système d'exploitation. En effet, on sait que tel logiciel fonctionnant sur un "Mac " ne peut fonctionner sous Windows, et vice-versa, à moins de disposer de versions spécifiques. Au sein même du monde Windows, il arrive que des applications écrites pour la version personnelle, Windows9x ou ME, soient incompatibles avec la version plus professionnelle, NT ou 2000.

Si à l'heure actuelle coexistent plusieurs systèmes d'exploitation hermétiques l'un à l'autre, que dire alors de la compatibilité des applications avec les systèmes du futur ? Le problème risque là d'être encore plus aigu.

2. Solutions techniques

a) La migration de données

Comme pour le support, la solution semble ici être apportée par la migration de données. En effet, au lieu de recopier "simplement " les données d'un support à l'autre, on peut également changer la structure du document afin de la rendre exploitable par les logiciels du moment.

---

[177] M. ANTOINE et Y. POULLET, " 'Vers la confiance' ou comment assurer le développement du commerce électronique ", in *Authenticité et informatique*, Bruxelles, Bruylant, 2000, p. 362.

[178] Citons comme simple exemple Microsoft et son traitement de texte dont les dernières moutures semblent " oublier " les formats précédents de document !

b) L'émulation

D'autres pistes sont aussi à explorer, telles que l'émulation. L'émulation consiste à restaurer virtuellement, sur une machine récente, l'environnement, même obsolète, dans lequel le document a été créé. Quand on sait que la machine émulatrice doit être environ dix fois plus puissante que la machine émulée, cette technique apparaît fort coûteuse à l'heure actuelle. Cependant, la montée en puissance exponentielle des (micro)processeurs atténue l'impact réel de ce rapport de 1:10. Quoiqu'il en soit, la technique de l'émulation doit être davantage étudiée et testée avant de décider s'il s'agit d'une solution praticable au problème de l'archivage électronique.

En réalité, l'émulation comme la migration présentent avantages et inconvénients, et il semble difficile de trancher arbitrairement en faveur de l'une ou de l'autre technique sans prendre en considération le type de document concerné [179]. Il convient d'abord d'examiner la dépendance du logiciel par rapport au matériel informatique, afin de voir si le document numérique peut être archivé indépendamment de l'environnement dans lequel il a été créé. Il faut également tenir compte de l'objectif poursuivi par l'archivage. La migration semble convenir davantage si le but est uniquement de retrouver et de consulter aisément des informations définitivement fixées. Par contre, l'émulation est préférable si l'on veut également préserver les outils nécessaires à une utilisation active des données (modification, ajout, suppression d'information...). Ajoutons enfin que l'émulation est une technique complexe qui nécessite le recours à des spécialistes, alors que la migration pourrait être opérée par les services d'archives eux-mêmes.

c) Vers un format d'archives universel et impérissable ?

Par ailleurs, une récente prise de conscience a conduit l'association française Aristote (composée de grands organismes de recherche : CNES, CEA, Inria, …) à créer, en juin 2000, le groupe de réflexion PIN (Pérennisation des informations) dont le but est la conception de formats d'archives universels et impérissables (ISO) à l'aide du standard XML. Notons qu'avec cette solution, le problème de la fragilité des supports reste entier.

XML, pour eXtensible Markup Language, est un format de description de données qui reprend le principe des balises HTML, mais en y ajoutant une grande souplesse, au contraire de son aîné. Si les balises HTML sont fixées par un organisme de normalisation (W3C), chacun est libre de créer son propre descripteur XML. En effet, chaque document XML d'un document nommé DDT reprend la sémantique des balises utilisées. Ainsi, nous nous retrouvons avec de simples fichiers texte, donc normalement interprétables facilement, qu'il suffit alors de corréler pour exploiter les informations qui y sont stockées. Le DDT est en quelque sorte la clé d'interprétation du XML.

C. Intégrité du contenu

Longtemps, le principal reproche adressé aux documents informatiques fut l'altérabilité de leur contenu. En effet, il est particulièrement aisé d'apporter des modifications au contenu d'un document numérique quelconque, de manière totalement imperceptible. La solution à ce problème réside aujourd'hui dans le recours à la signature numérique, dont une des fonctions, on l'a dit, est de préserver l'intégrité de l'acte signé.

[179] Pour une analyse détaillée de la question, voy. F. BOUDREZ, *op. cit*., pp. 8 à 12.

Lorsqu'on entend veiller au maintien de l'intégrité d'un document tout au long de son existence, il faut être attentif aux finalités de la conservation dudit document.

Dans certains cas, il peut s'agir de conserver intact un document, de telle manière que son contenu ne puisse subir aucune altération ou modification par la suite. Il faut alors figer définitivement le contenu du document, de telle manière que seule sa consultation soit possible, sans qu'aucun changement quelconque puisse y être apporté. Cette fonction d'intégrité peut être remplie tantôt par le support du document (papier, CD-ROM…), tantôt par le recours à la signature électronique.

Dans d'autres cas, il faut conserver un document qui peut ou doit encore subir des modifications par la suite : mentions marginales, ajout de pièces au dossier, etc. Il s'agit alors de garantir que chacune des modifications ultérieures sera repérable et datable (*infra*, point IV).

On le voit, il convient de se garder d'une approche trop étroite de la conservation de documents, en la confinant dans une stricte fonction d'intégrité.

D. Confidentialité

Il peut encore s'avérer important de garantir la confidentialité des données stockées. Ici, il semble que le support informatique se montre plus adéquat que le support papier. En effet, si l'accès peut y être facilité par des techniques efficaces de recherche, il peut également être aisé de crypter les données confidentielles, les rendant ainsi accessibles uniquement aux porteurs de la clé de cryptage adéquate.

Se pose aussi le problème de l'effacement de données que l'on ne désire plus conserver. En effet, dans la plupart des cas, effacer un fichier est une opération rapide, mais seule la *référence* à ce fichier est supprimée. Dès lors, il est toujours possible de parcourir exhaustivement le support (non réécrit) pour y retrouver le fichier effacé. Cependant, il existe des logiciels assurant la destruction réelle du fichier (la zone où il est stocké est réinitialisée), ou des fonctions *ad hoc* des logiciels courants.

IV. L'HORODATAGE DE DOCUMENTS ÉLECTRONIQUES

La question de la conservation de documents sous forme électronique est étroitement liée à celle de leur horodatage. Aussi, nous nous penchons à présent sur les moyens techniques d'horodatage existants et fiables (A) et sur l'importance de (horo)dater les documents électroniques d'un point de vue juridique (B).

A. Aspects techniques

On parlera d'horodatage de documents, ou *timestamping* en anglais, pour désigner l'association d'un message électronique à un moment déterminé[180].

Tout système d'exploitation affecte une date de création, voire d'accès, à un fichier qu'il gère. Mais cela n'est guère fiable, ni attaché au document. En effet, tout un chacun peut aisément modifier l'heure de son ordinateur personnel, voire corriger directement la date associée à un fichier. De plus, cette date est affectée par le système pour sa propre gestion des fichiers : un document recopié d'ordinateur à ordinateur verra probablement sa date modifiée au gré des recopiages (chaque système lui affectant sa propre date). Il en va de même en ce qui concerne le courrier électronique, où une date précise et incontestable revêt une certaine importance.

Depuis quelques années déjà, la question de l'horodatage de documents est à l'étude, mais les solutions proposées reposent toutes sur le même principe de base, qui est celui de la signature électronique, largement étudiée par ailleurs.

Rappelons brièvement le fonctionnement de cette dernière. Une telle signature se base sur un cryptage à clés asymétriques (clé privée + clé publique), ainsi que sur des algorithmes dits de "hash" qui sont des fonctions à sens unique calculant un condensé du fichier qui leur est soumis, condensé qui ne peut être "décodé" : il n'existe, à partir de ce condensé, aucun moyen de retrouver le fichier qui a servi de base à sa génération. L'authenticité du document est prouvée en recalculant le "hash" à partir du fichier lui-même, et en confrontant sa valeur à celle reçue initialement. Ainsi donc, pour signer un document et en garantir, en sus de l'origine, l'authenticité, l'apposition d'une signature électronique à un document se fait en réalité sur le "hash" obtenu pour ce document après application d'un algorithme de cryptage. Ainsi, lorsque le destinataire reçoit le document signé, son logiciel procède à la vérification de la signature en recalculant le "hash", et en le comparant avec celui reçu (après décryptage, bien entendu). Pour garantir la validité de la signature en elle-même, on l'associera vraisemblablement à un certificat émis par un tiers certificateur ou autorité de confiance.

Ce système à clés, "hash" et tiers certificateur fonctionne bien dans le contexte de la signature électronique. Dès lors, l'idée est venue de reprendre le même schéma de fonctionnement pour garantir une date associée à un document. Dans ce cas, au lieu d'avoir affaire à un tiers certificateur de signature, nous aurons affaire à un tiers certificateur de temps, c'est-à-dire que ce tiers émettra un certificat garantissant que tel document, dont voici le "hash", a bien été soumis à certification à telle date, telle heure.

Reste la question de la validité universelle de l'horodatage émis par telle ou telle autorité (on parlera également de *timestamp*, en utilisant le terme anglo-saxon). Pour ce faire, on peut

[180] T. PIETTE-COUDOL, *Echanges électroniques, certification et sécurité, op. cit.*, p. 145.

évidemment se baser sur le Temps Universel, et ne pas tenir compte des fuseaux horaires. Reste alors à l'autorité à obtenir un TU qui soit véritablement "universel" et non contestable.

Pour ce faire, la meilleure solution consiste à faire en quelque sorte la moyenne des temps référencés par plusieurs serveurs spécialisés dans le monde : observatoires astronomiques, US Navy…

Le protocole Internet X.509 *Public Key Infrastrucure* a été étendu par un *Time Stamp Protocol*[181]. Aux termes de celui-ci, un tiers horodateur (ou *Time Stamping Authority* ou TSA) doit se conformer aux points suivants :

- utiliser une source de temps fiable,
- inclure pour chaque marque de temps une valeur de temps fiable,
- inclure un entier unique pour chaque marque de temps nouvellement générée,
- produire une marque de temps à la réception d'une requête valide de la part du requérant, lorsque c'est possible,
- inclure avec chaque marque de temps un identifiant pour indiquer de manière unique la politique de sécurité sous laquelle la marque de temps a été produite,
- ne marquer que le "hash" représentant le document, c'est-à-dire une empreinte associée à une fonction de hash à sens unique, résistante aux collisions et identifiée de manière unique par un OID[182],
- examiner l'OID de la fonction de hash à sens unique et résistante aux collisions, et vérifier que la longueur de valeur du hash est cohérente avec l'algorithme de hash,
- n'examiner en aucune façon l'empreinte à marquer temporellement (sauf pour se conformer au point précédent),
- ne pas inclure d'identification quelconque de l'entité requérante des marques de temps,
- signer chaque marque de temps en utilisant une clé générée exclusivement à cet effet et avoir la propriété de cette clé indiquée sur le certificat correspondant,
- inclure des informations additionnelles dans la marque de temps, si demandé par le requérant en utilisant des champs d'extension, uniquement pour les extensions supportées par la TSA. Si cela n'est pas possible, la TSA *doit* répondre par un message d'erreur.

Ce dernier point se réfère au formalisme des messages échangés entre requérant et TSA pour obtenir l'horodatage d'un document, formalisme que nous n'aborderons pas ici.

Le protocole X.509 utilisé pour horodater des documents est utilisé notamment par Microsoft dans ce cadre.

Ainsi donc, pour horodater un document, il convient de soumettre celui-ci à la certification d'un tiers de confiance qui émettra un certificat contenant deux éléments importants : le "hash" du document, et la marque de temps associée.

Il est important de noter que l'horodatage d'un document peut se faire tout en maintenant la confidentialité de celui-ci. En effet, le tiers de confiance n'a pas à ouvrir le document pour lui associer une marque de temps. Dès lors, si l'on veut garantir la confidentialité du document envoyé au tiers horodateur, il suffit de le signer numériquement, ce qui n'entravera en rien la tâche de l'horodateur.

[181] © ISOC 1999, work in progress [version 14, avril 2001]
[182] Object IDentifier

B. Aspects juridiques

La datation d'un document revêt une importance certaine en droit[183]. La mention d'une date peut être une exigence légale (1). A certaines conditions, un document peut se voir reconnaître date certaine (2). Enfin, la date d'un acte est souvent le point de repère pour faire jouer les termes et les délais (3).

1. La mention de la date

Dans de nombreuses hypothèses, la loi exige la mention d'une date.

a) Examen de quelques dispositions

Souvent, l'apposition d'une date doit être faite par une autorité publique (officier public, administration).

Parmi les textes qui exigent l'apposition d'une date, citons, entre autres :

- art. 720 C. jud. : "Un dossier est constitué pour toute cause inscrite au rôle général.
  Le greffier inscrit sur la chemise du dossier la date de la mise au rôle et le numéro d'ordre de la cause."
- art. 755 C. jud. : "Les parties ou leurs avocats peuvent décider conjointement de recourir à la procédure écrite. En ce cas, ils déposent au greffe leurs mémoires, notes, pièces et conclusions préalablement communiqués, enliassés et inventoriés. Il leur en est donné récépissé à la date du dépôt."
- art. 769, al. 2, C. jud. : "Le juge peut autoriser les parties ou leurs avocats à déposer leurs dossiers au greffe, contre récépissé daté, après les débats et dans le délai qu'il fixe."
- art. 1027 C. jud. : "[La requête unilatérale] est déposée au greffe, visée à sa date par le greffier, inscrite dans le registre des requêtes et versée au dossier de la procédure. Elle peut aussi être adressée sous pli par l'avocat au greffier."
- art. 1099, al. 1er, C. jud. : "Le greffier constate la remise des requêtes et mémoires au moyen de notes marginales, qu'il signe en indiquant la date de réception."

Quelque fois, la mention de la date est exigée *ad solemnitatem*, c'est-à-dire qu'elle fait partie des mentions obligatoires de l'*instrumentum*.

- acte notarié : "Les actes énoncent également les noms, prénoms usuels et domicile des témoins prévus aux articles 10 et 11, ainsi que le lieu et la date où les actes sont passés." (art. 12, al. 2, de la loi du 25 ventôse an XI contenant organisation du notariat) ;
- exploit d'huissier : "A peine de nullité, l'exploit de signification doit être signé par l'huissier de justice instrumentant et contenir l'indication : 1° des jour, mois et an et du lieu de la signification (…)" (art. 43 C. jud.) ;

La date doit parfois être apposée par le ou les auteurs de l'acte eux-mêmes :

- testament olographe : "Le testament olographe ne sera point valable, s'il n'est écrit en entier, daté et signé de la main du testateur; il n'est assujetti à aucune autre forme." (art. 970 C. civ. – mention requise à peine de nullité : art. 1001 C. civ.) ;

[183] Pour une analyse détaillée du rôle de la date en droit, voy. B. SOUSI-ROUBI, " Variations sur la date ", *Rev. trim. dr. civ.*, 1991, pp. 70 et s.

- contrat de crédit à la consommation : "Le consommateur doit faire précéder sa signature de la mention manuscrite et en toutes lettres : 'lu et approuvé pour ... francs à crédit.' Il doit y apporter également la mention manuscrite de la date et de l'adresse précise de la signature du contrat" (art. 17 de la loi du 12 juin 1991 relative au crédit à la consommation) ;
- contrat d'assurance terrestre : "Le contrat d'assurance mentionne au moins : 1° la date à laquelle le contrat d'assurance est conclu (…)" (art. 10, § 2, de la loi du 25 juin 1992 sur le contrat d'assurance terrestre) ;
- voy. également la lettre de change, le billet à ordre, le chèque, etc.

L'omission de la date peut, dans certains cas, entraîner la nullité de l'acte. C'est le cas, on l'a vu, des exploits d'huissier, des testaments olographes ou encore du contrat de crédit à la consommation. Citons encore l'article 862, 3°, du Code judiciaire, qui prévoit que le juge peut déclarer nul un acte de procédure, sans vérifier l'existence d'un grief dans le chef de la partie qui invoque l'exception, lorsque la date de l'acte est omise, alors que cette indication est nécessaire à l'appréciation des effets de cet acte[184].

b) L'exigence de la mention d'une date dans un contexte numérique

Dans un univers papier, la mention de la date signifiait, par la force des choses, une inscription (manuscrite, dactylographiée, au moyen d'un cachet…), apposée sur l'acte à dater, c'est-à-dire sur le papier.

Dans l'environnement numérique, on se demande si cette conception de la mention de la date ne pourrait pas être envisagée sous une autre forme, dématérialisée, celle-là. La réflexion menée ici n'est pas sans évoquer les débats qui ont eu lieu à propos de la signature. Il est d'ailleurs intéressant de noter que dans de nombreuses hypothèses, date et signature sont étroitement liées, la première devant précéder la seconde. Or, l'examen des techniques d'horodatage de documents électroniques (*supra*, point A) renforce ce parallèle entre signature et date, l'horodatage étant fondé sur une technique analogue de *hashing* et de certification.

Selon cette conception évolutive, on pourrait admettre que l'exigence légale de la mention d'une date soit satisfaite par un système d'horodatage électronique, à condition que celui-ci présente toutes les garanties de fiabilité.

Toutefois, un tel système ne s'avérera pas adéquat dans toutes les hypothèses où la date de l'acte doit être indiquée. En effet, si les parties décident d'antidater ou de postdater l'acte, on ne peut envisager le recours à un système d'horodatage, celui-ci attribuant au document électronique une date et une heure correspondant précisément au moment où l'horodatage a lieu. Dès lors, ce n'est que dans l'hypothèse où la date à apposer est précisément celle du jour de l'apposition qu'un système d'horodatage est envisageable.

Dans tous les cas où la date à mentionner ne correspond pas au moment où la mention est apposée, on envisagera alors *l'inscription* de la date *dans le contenu* de l'acte électronique lui-même. Dès lors, l'intégrité de la date sera tributaire d'un système garantissant l'intégrité du contenu du document électronique (voy. *supra*, point III.C).

[184] Sur cette disposition, voy. A. FETTWEIS, *Manuel de procédure civile*, 2e éd., Faculté de droit de Liège, 1987, n° 143, p. 133.

2. La date certaine

a) Principes

Lorsqu'elle est apposée sur un acte sous seing privé par les parties, la date fait foi jusqu'à preuve du contraire (art. 1322 C. civ.). Vis-à-vis des tiers, une telle date ne sera opposable que si elle a valeur de date certaine.

L'article 1328 du Code civil fixe les circonstances dans lesquelles un acte sous seing privé a date certaine : "Les actes sous seing privé n'ont de date contre les tiers que du jour où ils ont été enregistrés, du jour de la mort de celui ou de l'un de ceux qui les ont souscrits, ou du jour où leur substance est constatée dans des actes dressés par des officiers publics, tels que procès-verbaux de scellé ou d'inventaire"[185].

L'existence d'une date certaine des actes peut également résulter de la rédaction d'un acte authentique. Ce dernier fait pleine foi de la convention qu'il renferme entre les parties contractantes et leurs héritiers ou ayants cause (art. 1319 C. civ.). Qu'il s'agisse d'un acte notarié, d'un exploit d'huissier ou d'un jugement, il atteste de son contenu, et notamment de sa date. La certitude de cette dernière est donc acquise.

L'acte sous seing privé n'offre pas les même garanties. En effet, il est rédigé par les parties, ce qui peut donner lieu à des falsifications. C'est pourquoi la certification de sa date par un tiers ou par un événement est imposée par l'article 1328 du Code civil.

b) La date certaine dans l'environnement numérique

A la lumière de ces développements, on constate qu'un acte peut acquérir date certaine par l'intervention d'un tiers[186]. Lorsqu'il s'agit d'un acte authentique, c'est l'intervention de l'officier public qui lui confère automatiquement date certaine. Lorsqu'il s'agit d'un acte sous seing privé, la date certaine de l'acte peut résulter, notamment, de son enregistrement.

En outre, c'est précisément au moment où ce tiers intervient que l'acte acquiert date certaine, et pas avant (antidate) ni après (postdate). On peut dès lors envisager le recours à un système d'horodatage de documents électroniques dans le but de lui conférer date certaine (cf. *infra*, point V.C). En effet, on l'a vu, la date apposée par un tel système correspond précisément au moment où l'horodateur intervient.

3. La date, les termes et les délais

Lorsqu'un acte est conclu sous un terme (suspensif ou résolutoire), la date de cet acte peut être prise en compte comme point de référence pour le début ou l'échéance du terme.

La date d'un acte joue également un rôle primordial pour l'ouverture ou l'expiration de certains délais, notamment les délais de procédure.

---

[185] Pour plus de développements, voy. F. FAVENNE-HERY, "La date certaine des actes sous seing privé", *Rev. trim. dr. civ.*, 1992, pp. 1 et s.

[186] On n'envisage pas ici la survenance d'un événement tel que le décès d'une des parties.

L'article 52, al. 1er, du Code judiciaire stipule que "*Le délai se compte de minuit à minuit. Il est calculé depuis le lendemain du jour de l'acte ou de l'événement qui y donne cours et comprend tous les jours, même le samedi, le dimanche et les jours fériés légaux.*"

Notons que l'article 52, al. 3, détermine la date d'un acte accompli par télécopie ou par courrier électronique au moment où il arrive, que le greffe soit ou non accessible au public à ce moment. Un telle disposition pose clairement la question de l'horodatage d'un courrier électronique. En effet, si un acte posé par e-mail parvient au greffe en dehors des heures d'ouverture, le moment de sa réception au greffe devra être attesté par un système fiable d'horodatage automatisé, à défaut de présence humaine. Cette question renvoie à la mise en place d'un recommandé électronique, attestant non seulement de la bonne réception d'un courrier électronique, mais également du moment précis de cette réception.

V. RECOMMANDATIONS, PISTES DE RÉFLEXION ET PROPOSITIONS DE TEXTES LÉGISLATIFS

A. L'évolution du formalisme et de la notion d'écrit au-delà du droit des obligations

La conservation de documents sous forme électronique n'a de sens que si le document conservé se voit reconnaître recevabilité et valeur probante lors de sa production en justice. Or, l'admissibilité des documents électroniques au titre de preuve ne fait plus de doute, au regard des lois "signature" et "certification", ainsi que des actuels travaux de transposition de la directive sur le commerce électronique (et plus spécifiquement son article 9).

En effet, afin de lever les obstacles (directs et indirects) à la conclusion de contrats par voie électronique, le législateur belge semble envisager l'adoption de différentes dispositions qui s'orientent indéniablement vers une approche fonctionnelle du formalisme dans les contrats.

Ainsi, une disposition transversale à caractère général est à l'étude dans le cadre de la transposition de la directive, afin de permettre une interprétation de la notion de formalité au sens large, détachée de toute forme et de tout support en particulier. Elle pourrait prendre la forme suivante :

"Lorsqu'il est exigé, au cours du processus contractuel, une formalité qui peut faire obstacle, directement ou indirectement, à la conclusion de contrats par voie électronique, celle-ci s'interprète indépendamment de sa forme et de son support. En toute hypothèse, les qualités fonctionnelles de la formalité considérée doivent être préservées".

D'autres dispositions transversales sont également envisagées, afin de prendre en considération les formalités les plus couramment exigées au cours du processus contractuel. C'est dans ce cadre que la définition suivante de l'écrit peut être proposée :

"Lorsqu'une disposition législative et réglementaire exige un écrit au cours du processus contractuel, cet écrit peut résulter d'une suite de lettres, de chiffres ou de tous autres signes intelligibles, accessible pour une consultation ultérieure, quels que soient son support et ses modalités de transmission".

Vu les travaux de transposition de la directive sur le commerce électronique, on semble s'orienter vers une définition de l'écrit libre de tout support et de toute forme, qui devrait présenter les qualités de lisibilité et de stabilité, mais non celle d'intégrité, étant entendu que cette fonction est le propre de l'écrit *signé*, sur le terrain probatoire.

Les dispositions ainsi envisagées concernent la levée des obstacles qui parsèment le "processus contractuel". Cette expression, on l'a dit, étend ses limites bien au delà de la simple étape de conclusion du contrat, puisqu'elle comprend la période précontractuelle, la conclusion proprement dite, l'exécution du contrat, son enregistrement, sa modification, la fin du contrat, mais aussi son archivage. Le champ d'application de ces dispositions est donc très vaste, et touche directement à la problématique de la conservation des contrats.

Toutefois, ces dispositions sont limitées au champ contractuel. En effet, la directive à transposer n'envisage pas le formalisme en dehors de la conclusion d'un contrat. Des

domaines tels que le droit fiscal[187], le droit comptable, ou le droit judiciaire, ne sont pas visés lorsque les formalités imposées ne sont pas liées à la passation d'un contrat.

En ce qui concerne cette dernière matière, on peut donc dire qu'il n'y a pas, à l'heure actuelle, de définition de l'écrit en droit judiciaire. Toutefois, dans la mesure où le débat se pose dans les mêmes termes qu'en droit civil[188], on pourrait en donner une définition comparable à celle proposée ci-dessus.

En outre, en ce qui concerne le cas précis de la conservation de documents, seul l'archivage des contrats est envisagé pour la transposition de l'article 9 de la directive sur le commerce électronique. Dès lors, il subsiste, dans de nombreuses autres matières, et notamment en droit judiciaire, des formalités susceptibles de faire obstacle, directement ou indirectement, à la tenue et à la conservation de certains documents par voie électronique. C'est pourquoi on examine au point suivant l'opportunité d'adopter une disposition générale en matière de conservation de documents.

B. La conservation de documents

A l'instar de la réflexion qui a été menée autour de la levée des obstacles formels à la conclusion de contrats par voie électronique, deux approches – non nécessairement exclusives l'une de l'autre – sont envisageables afin de permettre la conservation de documents sous forme électronique. Il s'agit, d'une part, de modifier, disposition par disposition, les multiples textes prescrivant la conservation de documents, lorsque leur formulation fait obstacle à une conservation sous forme numérique, d'autre part, d'adopter une disposition transversale qui couvrirait l'ensemble des textes législatifs et réglementaires.

L'approche consistant à adapter les textes légaux, disposition par disposition, présente l'avantage de permettre l'introduction de modifications sur mesure en fonction des différentes formalités prescrites et des objectifs poursuivis par chacune d'entre elles. On a vu, en effet, que certains documents à conserver ont été envisagés par les textes légaux dans un environnement papier. Ainsi, on retrouve des termes tels que "chemise", "feuille", "marge", "enliassés", mais aussi des exigences formelles telles que l'inscription "sans blanc ni interligne" ou la numérotation ou le paraphe de chacune des pages d'un document.

"Néanmoins, pareille entreprise présente au moins deux inconvénients majeurs : tout d'abord, elle nécessite un inventaire complet de l'ensemble des dispositions éparses dans notre arsenal législatif et réglementaire, ce qui représente une tâche considérable et fastidieuse, voire impossible dans un délai raisonnable, sans compter le risque de manquer certaines d'entre elles ; ensuite, ce type d'approche n'est pas de nature à assurer la cohérence d'ensemble des modifications. Dans la mesure où elle serait la seule adoptée, cette approche ne semble pas adéquate"[189]. Néanmoins, elle pourrait s'avérer d'une utilité certaine afin de combler les éventuelles, voire inévitables, lacunes liées à l'adoption d'une disposition transversale, qui ne pourra certainement pas couvrir la totalité des modalités de conservation envisagées par la loi.

---

[187] Cette matière est d'ailleurs expressément exclue du champ d'application de la directive sur le commerce électronique (art. 1er, 5, a).

[188] G. DE LEVAL, H.-P. GODIN et D. MOUGENOT, "Le code judiciaire à l'épreuve du cyberespace : la nécessaire réforme", in *Multimédia – Le cyberavocat*, Liège, Formation permanente CUP, vol. XXIX, 1999, p. 400.

[189] D. GOBERT et E. MONTERO, Cahiers du CRID, n° 19, *op. cit.*, p. 241, n° 442, à propos des approches législatives les plus adéquates pour lever les obstacles formels à la conclusion de contrats par voie électronique.

La seconde approche consisterait à prévoir une disposition transversale envisageant l'exigence de conservation indépendamment de la forme et du support du document. Il faudrait en outre déterminer les garanties qui devront être remplies afin de maintenir un niveau de sécurité juridique comparable.

En réalité, l'efficacité comande de combiner les deux approches, en adoptant une disposition transversale relative à l'exigence de conservation, tout en prévoyant une délégation au Roi[190] pour opérer des modifications spécifiques à mesure que serait relevé un obstacle à la conservation de documents sous forme électronique. On aboutirait ainsi à une solution équilibrée, tenant compte à la fois des impératifs de sécurité juridique et de faisabilité de la réforme.

Lorsqu'une disposition légale ou réglementaire impose la conservation d'un document, elle envisage évidemment qu'il soit possible de consulter celui-ci ultérieurement. L'exigence d'une accessibilité du document pour une consultation ultérieure recouvre à la fois les conditions de stabilité et de lisibilité du document, tout en s'alignant sur la définition de l'écrit.

Rappelons que la durée pendant laquelle le document doit être accessible pour être consulté ultérieurement est très variable. Dès lors, les moyens à mettre en œuvre pour garantir l'accessibilité ultérieure à un document électronique ne sont pas de la même envergure lorsqu'il s'agit de le conserver 5 ans ou 50 ans. C'est pourquoi il conviendrait de préciser dans la loi que la période d'accessibilité doit être adaptée aux exigences légales en matière de conservation.

Quant à l'exigence d'intégrité, il faudra tenir compte du fait que certains documents conservés peuvent ou doivent subir des modifications au cours de leur existence. Il conviendra donc de distinguer ces deux situations dans la loi.

Si l'on veut que ces garanties d'accessibilité et d'intégrité soient vérifiables, il convient également d'imposer la conservation d'un certain nombre d'informations, telles que les informations relatives aux outils de cryptage, aux signatures numériques et aux certificats qui les accompagnent.

Nous proposons dès lors une disposition transversale du type suivant :

"§ 1er. - Lorsqu'une disposition législative ou réglementaire exige la conservation d'un document, cette exigence est satisfaite quels que soient la forme et le support du document, pour autant que :

- *le contenu du document soit accessible pour une consultation ultérieure, durant une période adaptée aux exigences légales et réglementaires en matière de conservation de documents ;*
- *le document soit conservé sous une forme garantissant l'intégrité de son contenu ;*
- *les données nécessaires à garantir l'intégrité et l'accessibilité du contenu du document et, le cas échéant, l'identité de son auteur, soient conservées.*

[190] Notons qu'un tel système de délégation au Roi est fréquemment utilisé pour opérer des modifications législatives de ce genre. Les arrêtés royaux doivent ensuite être confirmés par une loi, faute de quoi il sont bien sûr sans effet, le Roi n'ayant normalement pas le pouvoir de modifier une loi.

Toutefois, lorsque des modifications peuvent ou doivent être apportées au document lors de sa conservation, celles-ci doivent apparaître clairement, par tout moyen approprié.

§ 2. – Sans préjudice du § 1er, le Roi peut adapter, sur proposition du ministre concerné, toute disposition législative ou réglementaire qui constituerait un obstacle à la tenue ou à la conservation de documents sous forme électronique.

Avant le 31 mars de chaque année, le Roi dépose à la Chambre des représentants un projet de loi visant à confirmer les arrêtés pris l'année qui précède en vertu de l'alinéa 1er. Les arrêtés qui ne sont pas confirmés dans les 9 mois du dépôt du projet de loi à la Chambre des représentants sont sans effet."

C. La datation de documents

A certaines conditions, le recours à un système d'horodatage permet de conférer à un document électronique une date fiable. Pour cette raison, il nous semble que la datation d'un tel document par ce procédé devrait être admissible, dans une approche fonctionnelle.

Toutefois, une interprétation stricte de l'exigence légale de datation des documents (mention ou inscription d'une date) pourrait conduire à écarter un tel procédé. En effet, lorsqu'on parle d'horodatage (ou *time stamping*) il ne s'agit pas d'inscrire une date dans le document électronique, mais de lui associer logiquement (et non plus physiquement) une marque de temps précise.

Dès lors, à l'instar de la signature électronique, la reconnaissance de l'horodatage électronique devrait être formulée dans une loi, afin de lever toute incertitude. Il ne pourrait donc être possible de déclarer irrecevable la preuve de la date d'un acte ou de tout autre document au seul motif qu'elle est établie par un procédé d'horodatage électronique.

Dans cette perspective, nous proposons l'adoption d'une disposition transversale prévoyant que :

"Lorsqu'une disposition législative ou réglementaire exige la mention ou l'inscription d'une date, cette exigence peut être satisfaite au moyen d'un procédé électronique de datation."

Il appartiendra alors au juge d'apprécier souverainement la force probante d'un tel système, en vérifiant que ce dernier permet de garantir la fiabilité de la date ainsi attribuée au document. Afin de faciliter la tâche du juge dans cette délicate entreprise, on pourrait prévoir dans une disposition spécifique à quelles conditions le juge peut avoir la certitude de la fiabilité de la date attribuée par horodatage. Une telle démarche est similaire à celle qui a été adoptée pour les signatures électroniques.

Ainsi, tous les systèmes de datation de documents électroniques seraient recevables en justice, mais seuls les systèmes d'horodatage qualifiés d'avancés se verraient automatiquement reconnaître valeur probante, entre les parties comme à l'égard des tiers. L'horodatage avancé consisterait en l'attribution d'une date à un document électronique, sur base d'un certificat qualifié répondant à des exigences légales et techniques précises et fourni par un prestataire de service de certification satisfaisant lui aussi à certaines exigences légales.

Grâce à l'intervention de ce tiers de confiance, un tel système d'horodatage avancé présente les mêmes garanties de fiabilité que l'apposition d'une date par un officier public ou la rencontre des conditions de l'article 1328 du Code civil. A notre avis, un document ainsi horodaté devrait se voir reconnaître date certaine par la loi.

Dans cette perspective, nous proposons l'adoption de deux dispositions :

- Article X : *"Sans préjudice de l'article 1328 du Code civil, le recours à un procédé d'horodatage électronique avancé confère à l'acte horodaté la valeur de date certaine"* (Il conviendrait bien entendu de définir minutieusement dans la loi ce qu'on entend par 'horodatage avancé') ;
- Article Y : *"L'article 1328 du Code civil est complété comme suit : « ou dans le cas prévu à l'article X de la loi du … »"*.

D. Le recours à la certification

Si le recours à un tiers de confiance semble s'imposer afin de garantir la fiabilité des procédés utilisés dans la conservation et l'horodatage de documents électroniques, une telle solution n'est pas sans soulever de nombreuses questions.

Ainsi, il est plus que probable que nombre de prestataires de services de certification qui investissent aujourd'hui le marché en matière de signature électronique se lancent demain dans l'archivage et l'horodatage de documents électroniques, offrant ainsi aux utilisateurs tout un éventail de services de certification.

Dès lors, dans un souci de cohérence, il serait judicieux, lors de l'élaboration du cadre juridique pour les services de certification en matière de conservation et d'horodatage, de poursuivre le processus législatif sur les traces de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification.

Toutefois, si l'on envisage la conservation et la datation de documents dans le cadre de la mission particulière de certaines professions, on peut s'interroger sur la possibilité ou sur l'opportunité de confier à un tiers certificateur le rôle d'archiver et d'horodater les documents électroniques. En effet, le notaire, le greffier, l'huissier, sont déjà des tiers par rapport aux parties. Dès lors, peut-on envisager qu'ils confient à leur tour à un autre tiers la tâche qui leur incombe de par la loi ?

Un autre problème qui se pose est celui de l'obligation de secret professionnel et de confidentialité qui pèse sur ces acteurs. Comment garantir le respect de leur obligation déontologique de discrétion, nécessaires à la confiance des parties, si les documents qui leur sont confiés passent entre les mains d'une tierce personne ?

Dans le prolongement du présent rapport intermédiaire et suite aux débats et réactions que nos recommandations susciteront, ces questions devront être étudiées notamment à la lumière de l'étude menée sur l'acte authentique électronique et en concertation avec les milieux concernés.

CHAPITRE III

L'ACTE AUTHENTIQUE ELECTRONIQUE

Table des matières

CHAPITRE III

L'ACTE AUTHENTIQUE ELECTRONIQUE

I. AUTHENTICITÉ ET ACTE NOTARIÉ

Il existe, sur le plan général, deux grandes familles d'actes authentiques :

a. Les actes des pouvoirs législatif, exécutif et judiciaire, posés par les détenteurs de ces pouvoirs agissant dans l'exercice de leurs fonctions ; ces actes ont par eux-mêmes forme authentique ;

b. Les actes que l'on qualifie en général de "ministériels" ; ces actes ne sont pas accomplis par les pouvoirs précédemment cités mais par des fonctionnaires publics ou officiers ministériels auxquels autorité a été déléguée à cet effet. On citera au premier chef, les actes des notaires ; appartiennent également à cette seconde catégorie, les actes des huissiers de justice et ceux des greffiers, qui sont plus spécialement qualifiés d'actes extrajudiciaires.

Au regard de l'étendue de cette *summa divisio*, et conformément aux objectifs de la "commission preuve", nous nous limiterons, pour ce rapport intermédiaire, à faire l'examen de l'impact des nouvelles technologies sur l'acte authentique notarié qui, dans notre système juridique, s'est vu attribuer une valeur probatoire particulière. Ceci constituera une première étape, qui ne manquera par d'être complétée, en vue d'un rapport final, par l'analyse d'autres types d'actes authentiques, tels que ceux des huissiers.

S'agissant des actes notariés, l'article 1er de la loi de Ventôse[191] dispose que "*les notaires sont des fonctionnaires publics établis pour recevoir tous les actes et contrats auxquels les parties doivent ou veulent faire donner le caractère d'authenticité attaché aux actes de l'autorité publique, et pour assurer la date, en conserver le dépôt, en délivrer des grosses et des expéditions*"

Cet article nous éclaire sur la source de l'authenticité ; celle-ci réside dans l'autorité publique. "*Stricto jure*, il ne devrait appartenir qu'au seul Pouvoir de faire des actes authentiques ; mais il est impensable qu'il puisse intervenir en toute matière et il peut donc, par voie de délégation conférée à certains fonctionnaires publics ou officier ministériels, confier cette mission dans des matières déterminées"[192]. La source de l'authenticité de l'acte notarié s'inscrit dans cette perspective ; elle réside, en effet, dans la délégation donnée par le Pouvoir au notaire à cette fin. Si les actes publics sont donc authentiques par eux-mêmes, les actes privés ne le sont que par l'intervention du notaire, qui peut leur conférer un "*caractère d'authenticité*".

Dès lors, en matière civile, la catégorie des actes authentiques dressés par les notaires, sont assimilés, sur le plan de l'authenticité, à des actes publics.

---

[191] Loi du 25 Ventôse – 5 germinal an XI (16 mars 1803) – loi contenant organisation du notariat, *Bull. 258*, n° 2440 ; *Pasin.*, p. 16.

[192] P. WATELET, *La rédaction des actes notariés*, avec collab. de M. RENARD-DECLAIRFAYT, Bruxelles, Larcier, 1980, p. 24.

A cet égard, l'article 1317 du Code civil dispose que : *"l'acte authentique est celui qui a été reçu par les officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises"*.

Le législateur n'a cependant pas pris le soin de définir l'authenticité. Pour préciser cette notion, il est éclairant, d'une part, de se référer au sens habituel du mot, d'autre part, d'observer les effets juridiques que la loi attache aux actes qu'elle reconnaît comme authentiques.

S'agissant de l'acception usuelle du mot[193], l'authenticité fait référence à "la qualité de ce qui est vrai", à ce dont "l'origine ne peut être contestée". L'étymologie du mot "authentique" permet de préciser cette notion et d'y trouver une référence à l'autorité, à ce "dont le pouvoir est inattaquable".

S'agissant des effets juridiques reconnus à l'acte authentique, il y a lieu de distinguer entre, d'une part un effet exécutoire, d'autre part, un effet probatoire. L'effet exécutoire de l'acte authentique est consacré par le Code Judiciaire, et précisé plus particulièrement, pour l'acte notarié, par l'article 19 de la loi de Ventôse.[194] En tant qu'acte émanant de l'autorité souveraine, le dispositif de l'acte authentique doit être réalisé, les obligations qui y sont souscrites doivent être exécutée, son but doit être atteint. Quant à l'effet probatoire, celui-ci est consacrée par le Code civil dans son système de preuve littérale. L'acte authentique doit pouvoir être cru. En raison de son caractère authentique, il ne peut être contesté (v. *infra* pt. II).

Dans ce contexte, "on peut déduire de ces prémices que l'authenticité est le caractère de vérité et de force qui s'attache aux actes de l'autorité publique. Il ne peut d'ailleurs pas en être autrement. Que vaudrait l'acte de l'autorité publique sans l'impossibilité pour le citoyen d'en contester la véracité et sans la possibilité pour le Pouvoir d'en imposer l'exécution même *manu militari* ? Si telles qualités n'étaient pas attachées à ses actes, le Pouvoir ne serait pas le pouvoir. On comprend alors que l'authenticité soit le propre des actes de l'autorité publique, que les actes qu'il pose en bénéficient par nature tandis que les actes privés doivent en être spécialement dotés, et ce, par le notaire, fonctionnaire public établi à cette fin"[195]

[193] *Dictionnaire de la langue française - Le Petit Robert*, Paris, Dictionnaires Le Robert, 1990, p. 133, v° Authentique.
[194] E. IEROY, "De la force exécutoire des actes notariés : principes, limites et perspectives", *Authenticité et Informatique*, Congrès des notaires, Bruxelles, Kluwer – Bruylant, 2000, pp. 77 et s.
[195] J. DEMBLON, "L'acte notarié", *Rép. Not.*, t. XI, Livre VII, n° 13.

II. AUTHENTICITÉ ET FORCE PROBANTE

A. Théorie de la preuve en droit privé

Dans nos systèmes juridiques de droit latin[196], la preuve écrite et préconstituée a acquis la prééminence, tout au moins en droit civil. Le législateur a en effet privilégié la preuve écrite rédigée à un moment où il n'existait pas encore de litiges entre parties dans le but de se constituer une trace des relations existant entre elles.

Parmi les modes de preuve écrite, le législateur a placé l'acte authentique en haut de la hiérarchie. Cette place privilégiée s'explique par la force probante légalement reconnue à ce type d'acte. Il convient de rappeler que, dans le cadre de ce rapport, nous ne traiterons que des actes notariés, ceux-ci occupant, en doit de la preuve, un rôle spécifique, voire prépondérant[197] parmi la diversité des actes authentiques[198]. Toutefois, les autres types d'actes authentiques (certains actes des fonctionnaires ou mandataires publics, les actes des huissiers, les actes de procédure accomplis par les magistrats et leurs greffiers) feront l'objet de développements dans le prochain rapport[199].

La matière de la force probante des actes notariés relève essentiellement, dans notre système juridique, du droit civil et plus particulièrement du droit des obligations.

Le siège de la matière se situe au Chapitre VI du Code Civil, consacré à la preuve des obligations ; c'est là que l'on trouve les articles 1317 à 1319 relatifs à l'acte authentique. L'acte notarié est donc un des modes de preuve légalement autorisé en droit civil, mais il bénéficie d'une force probante privilégiée, particulière. Il constitue la première preuve, la plus sûre et la plus complète.

Quelles sont les raisons de statut privilégié et quelle en est la portée ?

Afin de mesurer de façon adéquate la force probante des actes notariés, il est utile, comme point de départ de s'attacher à leur définition. L'acte notarié peut être défini de la manière suivante : "l'acte notarié est le document écrit, établi par notaire, au titre d'acte instrumentaire avec caractère d'authenticité"[200]

Cet acte est qualifié d'instrumentaire dans la mesure où il est établi pour servir d'instrument de preuve. Mais la caractéristique principale de l'acte notarié réside dans sa force probante, dans le degré de crédibilité qui y est attaché. Ainsi, pour être qualifié d'acte notarié, l'écrit établi par le notaire à des fins probatoires doit être pourvu par lui du caractère authentique. C'est du caractère d'authenticité qui lui ainsi conféré que l'acte notarié tire sa force probante exceptionnelle. Les notaires doivent alors être considérés comme les officiers publics compétents pour les actes destinés à faire preuve entre parties[201].

---

[197] R. MOUGENOT, *Droit des obligations. La preuve*, tiré à part du *Répertoire Notarial*, 2ème éd., Bruxelles, Larcier, 1997, n° 86-1.
[198] Remarquons d'ailleurs qu'une grande majorité des auteurs belges et français ne font référence qu'à ces seuls actes (notariés) lorsqu'ils traitent des actes authentiques.
[199] Notons d'ores et déjà qu'une grande part des développements de la présente étude relatifs à la force probante s'applique à l'ensemble des actes authentiques.
[200] Définition proposée par J. DEMBLON, *op. cit*, t. XI, Livre VII, 1991, p. 79.
[201] DE PAGE, t. II, 3ème éd., 1967, n° 753-754.

B. L'étendue de la force probante de l'acte notarié

Selon les termes de l'article 1319 du Code civil, *"L'acte authentique fait pleine foi de la convention qu'il renferme entre les parties contractantes et leurs héritiers ou ayants cause.*

Néanmoins en cas de plaintes en faux principal, l'exécution de l'acte argué de faux sera suspendue par la mise en accusation ; et, en cas d'inscription de faux (…), les tribunaux pourront, suivant les circonstances, suspendre provisoirement l'exécution de l'acte".

L'article 1320 du Code civil dispose en outre que : *"L'acte, soit authentique, soit sous seing privé, fait foi entre les parties, même de ce qui n'y est exprimé qu'en termes énonciatifs, pourvu que l'énonciation ait un rapport direct à la disposition. Les énonciations étrangères à la disposition ne peuvent servir que d'un commencement de preuve*".

Enfin, l'article 19 de la loi du Ventôse dispose que : *"Tous les actes notariés feront foi en justice et seront exécutoires dans toute l'étendue de la République*".

Sur le plan du droit de la preuve, ce statut privilégié de l'acte notarié[202] a pour conséquence qu'il ne peut être contesté que par la mise en œuvre de la difficile procédure d'inscription en faux. Revêtu de l'authenticité, l'acte notarié fait foi de son origine, il est vrai par lui-même. Dès lors, aucune preuve ne doit corroborer son authenticité, il bénéficie d'une présomption d'authenticité. "Le notaire est ainsi un témoin privilégié 'cru sur parole', en l'espèce 'cru sur son écrit'. Sont ainsi considérés comme certains, comme acquis, les faits rapportés par le notaire (…)"[203].

Cette qualité probatoire exceptionnelle a pour conséquence d'opérer un renversement de la charge de la preuve. Le titulaire de l'acte n'a rien à prouver ; c'est celui à qui on l'oppose à en contester la force probante.

Toutefois, la qualité de la force probante attachée au témoignage du notaire varie selon qu'il s'agit des constations faites par lui ou de la simple relation des déclarations faites par les parties en sa présence. En effet, est prouvée jusqu'à inscription de faux, la matérialité des faits et des déclarations dont le notaire affirme avoir une connaissance personnelle pour les avoir vus, entendus ou accomplis *ex propriis sensibus*.

Par contre, la véracité des faits ou actes juridiques déclarés par les parties, elle, n'est pas vérifiable. Dès lors, ces éléments ne sont pas protégés par l'obligation de recourir à la procédure de l'inscription en faux pour les contester. C'est en ce sens que *"acte authentique fait pleine foi de la convention qu'il renferme*" ; il fait pleine foi du fait de la déclaration de cette convention mais non de la véracité et de la sincérité du contenu de la déclaration.

C. La source de la force probante de l'acte notarié

Comme on l'a déjà souligné, la source de la force probante de l'acte notarié est l'authenticité. L'authenticité des actes privés a en effet été considérée comme indispensable à la vie en société ; c'est là la justification de l'authenticité des actes notariés. "Les nécessités sociales

[202] M. RENARD-DECLAIRFAYT, "Force probante des actes notariés", *Rép. Not.*, t. XI, Livre VI (1ère partie), 1991, p. 51. " 'Provision est due au titre'… : l'expression donne la mesure de la force probante qui émane de l'acte notarié".
[203] J. DEMBLON, "Organisation et déontologie du notariat", *Rép. Not.*, t. XI, Livre V, p.53.

exigent que dans les rapports entre les citoyens, ou dans les rapports entre citoyens et certaines institutions publiques ou privées, il existe des instruments probatoires dont la régularité formelle implique une présomption irréfragable de vérité. Par avance, toute erreur et toute surprise doivent être écartées ; il faut rendre impossible toute dénégation d'écriture et de signature ; aucune contestation ne doit pouvoir surgir"[204] Le notaire a donc, à cet égard, un rôle essentiel à jouer dans le domaine des relations privées. Par sa fonction, il assure la paix dans les relations sociales en prévenant les différends. Il ne doit pas trancher un litige unique et déterminé, il doit les prévenir en assurant la solidité juridique de l'acte qu'il reçoit. Le notariat apparaît ainsi comme une fonction de première ligne et de sécurité[205].

Pour bénéficier de l'authenticité, l'acte privé doit être reçu par *"un officier public"* compétent et *"avec les solennités requises"*. L'intervention du notaire ainsi que le respect de formalités sont les deux composantes de l'authenticité[206].

1. La fonction instrumentaire du notaire et le formalisme

La fonction notariale est de son essence première constituée d'une mission d'authentification. Il s'agit d'une mission dont est chargé le notaire par le Pouvoir afin de donner un caractère d'authenticité aux actes ; on peut la décrire comme une fonction "instrumentaire"[207].

En vertu de l'article 1317 du Code civil, l'acte doit être reçu avec *"les solennités requises"*. Il doit en effet répondre à diverse exigences de formes qui sont les gardiennes de l'ordre juridique.

La réalisation de l'acte notarié est subordonnée au respect d'un ensemble de formalités légalement définies. A cet égard, chaque fois que la loi évoque les formalités nécessaires à la réalisation de l'acte notarié, il est recouru au terme "recevoir"[208]. La réception d'un acte par notaire recouvre un sens bien particulier, même si ni la loi de Ventôse, ni le Code civil n'en fournissent la signification.

M. RENARD-DECLAIRFAYT en propose une définition, ou plutôt énumère les différentes formalités qui en font partie :"Au sens légal, la réception de l'acte notarié n'est pas autre chose que la constatation solennelle faite par le notaire de la comparution des parties, de l'émission de leurs volontés, de l'adhésion de chacune d'elles au contenu de l'acte, de leurs signatures, enfin de la date de l'acte, le tout suivant les règles de la loi de Ventôse. La signature du notaire est l'opération finale et décisive qui imprime force de loi à l'acte des parties"[209]

---

[204] P. WATELET, *op. cit.*, p. 23.
[205] P. HARMEL, préface à *La rédaction des actes notariés*, par P. WATELET, Bruxelles, Larcier, 1980, p. 11.
[206] M. RENARD-DECLAIRFAYT, *op. cit.*, pp. 43 et s.
[207] J. DEMBLON, *op. cit*, t. XI, Livre V/1, p. 50, n°10. L'adjectif "instrumentaire" souligne le fait que l'authenticité concerne l'*instrumentum* seul ; elle ne concerne en rien le *negotium.* Sous réserve de l'exception que constituent les actes solennels, sur le plan probatoire, *negotium* et *instrumentum,* sont indépendants : chacun subsiste indépendamment de la validité ou de la non-validité de l'autre.
[208] R. MOUGENOT, *op. cit.*, n° 85. Selon l'auteur, l'emploi du terme "recevoir" n'est pas très heureux. "Il s'explique par le fait que les auteurs du Code civil, en traitant de l'acte authentique, avaient continuellement à l'esprit l'intervention du notaire (…). Il existe cependant de nombreux actes authentiques où les chose se passent différemment. Un huissier de justice ne 'reçoit' rien lorsqu'il signifie une citation à comparaître en justice ou dresse un procès-verbal de saisie".
[209] Définition proposée M. RENARD-DECLAIRFAYT, *op.cit.*, n° 13 et 14. Voir également du même auteur, "La preuve devant le juge en droit privé, pénal et administratif. L'acte notarié, ses annexes et copies en tant que

La réception de l'acte notarié comprend généralement :

- la comparution et l'identification des parties ;
- l'intervention des témoins lorsqu'elle est requise ;
- la constatation de la date et du lieu de réception de l'acte ;
- la lecture de l'acte aux parties ;
- la signature par les parties et la mention de cette signature ;
- le tout s'effectuant en la présence permanente du notaire qui signe ensuite.

L'authenticité est ainsi basée sur l'intervention du notaire, plus précisément sur les constatations et affirmations que doit faire personnellement le notaire, les attestations qu'il doit fournir, le témoignage qu'il doit porter à l'occasion de la réalisation de l'acte : ce sont les solennités[210]. Celles-ci résultent toutes de la loi organique de Ventôse et exclusivement d'elle, elles sont dénommées comme telles dans la mesure où leur absence entraîne, pour la plupart d'entre elles, la nullité de l'acte ou son inexistence.

Ainsi considérée, la notion de "réception" correspond à l'intervention du notaire *qualitate qua* ; elle correspond à la seule fonction instrumentaire. En effet, il s'agit de "*donner aux actes et aux contrats le caractère d'authenticité attaché aux actes de l'autorité publique*" (Article 1er de la loi de Ventôse). A cette fin, le notaire doit respecter les règles de formes établies par la loi organique, en les interprétant dans l'optique de l'authenticité à atteindre.

Toutefois, il semble qu'on ne peut prendre adéquatement toute la mesure de la notion de "réception" en faisant abstraction de la fonction conseillère du notaire.

2. La fonction conseillère du notaire.

La fonction notariale est également constituée d'une mission de conseil. Il s'agit d'une mission dont est chargé le notaire, cette fois par les citoyens, afin de les éclairer sur la portée de leurs engagements ; on peut la dénommer fonction "conseillère"[211].

Il est aujourd'hui unanimement reconnu que ces deux fonctions incombent au notaire, même si elles n'étaient pas, à l'origine, toutes deux prévues par la loi. La loi organique en effet ne disait mot sur la fonction de conseil mais les travaux préparatoires et notamment l'exposé des motifs du conseiller REAL y faisaient référence[212]. Le notaire y était notamment décrit comme un "conseil désintéressé des parties…régulateur des engagements qu'ils veulent contracter". La source de l'obligation de conseil résidait, en définitive, dans la jurisprudence qui s'était plu à reconnaître "qu'un donneur d'authenticité automatique est d'une utilité sociale discutable s'il ne s'accompagne d'un conseiller judicieux et désintéressé, prêt à éclairer les parties sur leurs devoirs, sur leurs obligations et sur leurs droits, tant vis-à-vis les unes des autres que de l'autorité (…)"[213]. Aujourd'hui, la réforme récente du notariat a mis l'accent sur la mission

---

moyen de preuve en droit belge", *Rev. jurid. et pol. indépendance et coopération*, La preuve devant le juge, XVII Congrès de l'I.D.E.F., 1985, pp. 461 et s.

[210] J. DEMBLON, *op. cit.*, t. XI, Livre VII, n°181.

[211] *Ibidem*, n°10.

[212] REAL, Exposé des motifs de la loi organique, voy. "Code du notariat", *Rép. Not.*, t. XI, Livre II. Certaines loi particulières y faisaient cependant déjà allusion : loi du 4 novembre 1969 sur le bail à ferme, lois des 29 mars 1962 et 22 décembre 1970 sur l'aménagement du territoire et de l'urbanisme, loi du 9 juillet 1971 réglementant la construction d'habitations et la vente d'habitations à construire ou en voie de construction.

[213] Voy. l'introduction générale de l'ouvrage de P. WATELET, *op. cit.*, p. 15.

sociale et informative du notaire. L'article 9 de la loi du Ventôse, modifié par la loi du 4 mai 1999, dispose en effet que : *"Le notaire informe toujours entièrement chaque partie des droits et des obligations et des charges découlant des actes juridiques dans lesquels elle intervient et conseille les parties en toute impartialité*".

Il est d'usage d'identifier, dans cette obligation de conseil, trois aspects[214]. D'abord, incombe au notaire le devoir d'éclairer les parties. Le notaire est investi d'une mission de confiance dont il doit répondre – cette fois, non à l'égard du Pouvoir comme dans sa mission d'authentification – mais à l'égard des parties. Cette confiance se fonde sur l'attente des clients que le notaire les guide. A cette fin, le notaire doit veiller à la validité juridique des actes dont il est le rédacteur, il doit suggérer aux parties une rédaction complète, claire et précise de leurs conventions, il doit encore éclairer les parties sur la portée de leurs engagements et les conséquences qui en découlent.

Ensuite, le notaire est tenu à un devoir d'investigation personnelle. Avant d'éclairer les parties, il va de soi que le notaire doit être lui-même informé. Pour parer à d'éventuelles erreurs, incompétences ou négligences des parties, il est indispensable que le notaire s'informe sur des éléments aussi essentiels que la véracité des informations qui lui sont communiquées par les parties, sur la capacité de celles-ci et qu'il s'attache à vérifier tous les documents requis pour la rédaction de l'acte.

Enfin, la loi ou l'usage impose au notaire diverses obligations complémentaires à la réception des actes, telles que les obligations imposées par les lois fiscales (enregistrement, notifications aux services des contributions directes et de la T.V.A.)…

A ce titre, le devoir de conseil et d'information qui pèse sur le notaire en tant qu'officier public participe de manière substantielle, à l'authenticité[215].

En effet, "ces deux fonctions ne sont pas remplies successivement dans le temps : d'abord le conseil, ensuite l'authentification ; au contraire, la fonction de conseil recouvre la fonction d'authentification en ce sens que la première précède, accompagne et suit la seconde"[216]. Dès lors, il est légitime d'interpréter la notion de réception au sens large. Une telle interprétation tiendrait compte de la fonction conseillère du notaire et comprendrait donc toutes les opérations qui permettraient la réalisation d'une authentification plénière.

Dans cette optique, une réception, envisagée au sens large, comprendrait : la participation à l'élaboration de l'acte juridique, la rédaction de l'acte instrumentaire, l'intervention du notaire *qualitate qua*, et le respect des prescriptions complémentaires prévues par la loi organique et les usages.

---

[214] R. DE VALKENEER, *Précis du notariat*, Bruxelles, Bruylant, 1988, p. 114, n° 190.
[215] E. LEROY, *op. cit.*, p. 87 ; voy. également J.-F. TAYMANS, "Authentification active et responsabilité notariale", in *Authenticité et Informatique*, Congrès des notaires (F.R.N.B.), Bruxelles, Kluwer – Bruylant, 2000, p. 210.
[216] J. DEMBLON, *op. cit.*, t. XI, Livre VII, n°19.

III. L'ACTE AUTHENTIQUE ELECTRONIQUE

A. Contexte actuel

Le droit des contrats et de la preuve a subi de grands bouleversements ces derniers temps : l'arrivée conjuguée de la signature électronique et du contrat immatériel.

1. La directive du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques modifie le régime de la preuve.

Un des objectifs majeurs de la directive est la reconnaissance juridiques des signatures électroniques[217]. Sur le plan probatoire, elle a pour conséquence que l'écrit électronique signé à l'aide d'une signature électronique sera désormais admis en preuve au même titre que l'écrit signé sur support papier, à condition que l'identité de la personne dont il émane soit assurée et que son intégrité soit garantie. Jusqu'à présent, sur le plan probatoire, l'écrit papier, assorti d'une signature manuscrite permettait de cristalliser l'accord des volontés. Mais désormais, "l'heure est venue pour l'écrit de s'émanciper de la tutelle du papier. La liberté d'épouser d'autres formes lui est aujourd'hui reconnue. La circonstance qu'il se présente sous une forme électronique ne lui fait pas perdre pour autant sa qualité d'écrit"[218].

Une telle directive consacre dès lors l'ouverture de la preuve littérale aux écrits sous forme électronique et, par là, nécessite que soit réévaluée les règles de la preuve littérale dans la mesure où est consacrée l'assimilation de l'écrit sur support électronique à l'écrit sur support papier.

En ce qui concerne l'acte authentique, la démarche adoptée par la directive appelle une observation. En effet, la directive ne couvre pas les aspects relatifs à la validité des contrats.

L'article 1er qui définit le champ d'application de la directive dispose que :

« L'objectif de la présente directive est de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique. Elle institue un cadre juridique pour les signatures électroniques et certains services de certification afin de garantir le bon fonctionnement du marché intérieur.

Elle ne couvre pas les aspects liés à la conclusion et à la validité des contrats ou d'autres obligations légales lorsque des exigences d'ordre formel sont prescrites par la législation nationale ou communautaire ; elle ne porte pas non plus atteinte aux règles et limites régissant l'utilisation de documents qui figurent dans la législation nationale ou communautaire. »

Il n'est donc pas demandé aux Etats membres de toucher aux éventuelles formalités requises *ad solemnitatem*, mais uniquement aux exigences *ad probationem*. [219] Bien que cette césure

[217] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, n° L 13 du 19 janvier 2000, pp. 12-20.
L'autre objectif majeur de la directive est la création d'un cadre légal pour l'activité des prestataires de service de certification.

[218] D. GOBERT et E. MONTERO, "L'ouverture de la preuve littérale aux écrits sous forme électronique", *J.T.*, 2001, p. 114.

[219] M. ANTOINE et D. GOBERT, "La directive européenne sur la signature électronique : Vers une sécurisation des transactions sur l'Internet", *J.T.D.E.*, avril 2000, n° 68, pp. 73 à 78.

ne se fasse pas, comme telle, entre acte authentique et acte sous seing privé, elle vise notamment les actes authentiques. On se rappellera en effet que lorsqu'un écrit est exigé *ad solemnitatem*, "la règle de preuve est, en quelque sorte, absorbée par la règle de forme"[220] ; l'écrit conditionne alors la validité du *negotium*. La reconnaissance de la signature électronique semble donc s'arrêter aux cas où l'écrit n'est exigé qu'à titre probatoire. Cette restriction n'est donc pas aussi limitée qu'elle n'y paraît, et bien qu'elle ne concerne pas les seuls actes authentiques, elle touche un nombre considérable de contrats pour lesquels les différentes législations demandent un écrit signé à peine de nullité. En effet, si notre droit des contrats est basé sur le principe du consensualisme, ce principe connaît de nombreuses exceptions [221]. En droit belge, on peut citer : les contrats solennels, (droit de la famille, mariage, adoption), les contrats pour lesquels le législateur impose la passation d'un acte authentique, sans qu'on puisse pour autant les qualifier de solennels (constitution et modification des statuts de sociétés), les contrats dont l'opposabilité aux tiers requiert la forme authentique (transcription dans les registres de conservation des hypothèques), et enfin, les contrats pour lesquels le législateur exige un écrit, indépendamment de toute question de preuve (contrat de crédit à la consommation, contrat d'assurance, contrat de travail à durée déterminée).

Le législateur européen a donc fait preuve de prudence. En effet, le formalisme des actes, spécialement des actes authentiques, se justifie par des principes fondamentaux de sécurité juridique ; un tel formalisme relève notamment du souci de protection des personnes lorsqu'elles contractent des engagements particulièrement importants[222]. Il ne s'agissait pas en effet de mettre sur un pied d'égalité ces deux types d'actes sans au préalable approfondir la réflexion.

Dans ces différents cas, la papier devrait donc conserver son monopole, du moins pour un certain temps. "Mais pour un temps seulement et probablement très court, car la toute fraîche directive européenne 'Commerce électronique' adoptée en mai 2000, destinée à constituer la charte des contrats en ligne pour le XXIe siècle, interdit aux Etats membres de mettre obstacle à la pleine reconnaissance des contrats électroniques" (v. *infra*, pt. 2).

En Belgique, la loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire transpose partiellement[223] la directive.

Le nouvel article 1322 du Code civil stipule notamment que :

"Peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien et l'intégrité du contenu de l'acte."

---

[220] R. MOUGENOT, *op. cit.*, p. 128, n° 81.

[221] J.-F. TAYMANS, "Recueillir et authentifier le consentement : l'expérience notariale confrontée à la certification électronique", *Le consentement électronique*, Actes du colloque des 23 et 24 septembre 1999, B. DE NAYER et J. LAFFINEUR (Eds), Droit et Consommation, Bruxelles, Bruylant, 2000, p. 351.

[222] E. CAPRIOLI, "Le juge et la preuve électronique", p. 6, disponible en ligne à l'adresse http://www.juriscom.net/uni/doc/20000110.htm.

[223] *M. B.*, 22 déc. 2000, pp. 42698 à 42699. Voir également la très récente loi du 9 juillet 2001, loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *M. B.*, 29 sept. 2001, p. 33070.

L'exposé des motifs précise que la modification apportée par la nouvelle loi est applicable à tous les actes sous seing privé, pour autant qu'ils ne soient pas soumis à une législation spécifique. Il en résulte que si une telle loi prévoit des dispositions particulières faisant obstacle à l'utilisation de la signature électronique, ces dispositions devront être respectées tant que la législation spécifique n'aura pas été adaptée.

Comme dit précédemment, la modification adoptée ne semble donc viser que les actes sous seing privé, à l'exclusion des actes authentiques. En effet, ni les dispositions de la loi ni l'exposé des motifs ne traitent de l'acte authentique. De plus, la définition fonctionnelle de la signature est intégrée dans l'article 1322 du Code civil relatif uniquement aux actes sous seing privé. Enfin, cette interprétation est confirmée par les mots « application du présent article », qui semblent d'ailleurs restreindre considérablement la portée de cette définition.

Il en résulte que tant que le législateur belge n'aura pas modifié clairement les règles relatives à l'acte authentique, comme l'a fait le législateur français, ce dernier ne pourra être électronique.

2. La Directive du 8 juin 2000 sur le commerce électronique

Parallèlement à la directive sur la signature électronique, on peut constater que la directive du 8 juin 2000 sur le commerce électronique exclut prudemment de son champ d'application les "*activités de notaire*".

L'article 1er, 5, d dispose en effet que :

"La présente directive n'est pas applicable:

(…)
d) aux activités suivantes des services de la société de l'information:
- les activités de notaire ou les professions équivalentes, dans la mesure où elles comportent une participation directe et spécifique à l'exercice de l'autorité publique,
- (…)".

Toutefois, comme le soulignent D. GOBERT et E. MONTERO, une autre disposition de la directive suggère, de façon implicite mais non moins certaine, que l'on ne pourra faire longtemps l'économie d'une réflexion approfondie sur le rôle du notariat dans la société de l'information[224].

L'article 9 prévoit, en effet, que :

"*1. Les Etats membres veillent à ce que leur législation rende possible les contrats par voie électronique. Les Etats membres s'assurent, notamment, que le régime juridique applicable au processus contractuel n'empêche pas l'utilisation effective des contrats par voie électronique ni ne conduise à priver d'effet et de validité juridiques de tels contrats pour le motif qu'ils sont passés par voie électronique.*

[224] D. GOBERT et E. MONTERO, "L'ouverture de la preuve littérale aux écrits sous forme électronique", *op. cit.*, p. 120.

2. Les États membres peuvent prévoir que le paragraphe 1 ne s'appliquent pas à tous les contrats ou à certains e eux qui relèvent des catégories suivantes:

a) (…)
b) les contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique ;
c) (…)

0 3. Les États membres indiquent à la Commission les catégories visées au paragraphe 2 auxquelles ils n'appliquent pas le paragraphe 1. Ils soumettent tous les cinq ans à la Commission un rapport sur l'application du paragraphe 2 en expliquant les raisons pour lesquelles ils estiment nécessaire de maintenir les catégories visées au paragraphe 2, point b), auxquelles ils n'appliquent pas le paragraphe 1."

La Commission entend donc laisser le temps aux Etats membres d'effectuer un examen en profondeur des «*contrats pour lesquels la loi requiert l'intervention de professions exerçant une autorité publique* », tel est le cas des contrats devant être conclus devant un notaire ou un officier public, donc les actes authentiques. En effet, il s'agit de déterminer au cas par cas, l'objectif poursuivi par chacune des formalités et d'évaluer comment ils pourraient assurer la réalisation de ces objectifs dans l'environnement électronique.

Le paragraphe 3 de la directive impose d'ailleurs aux Etats membres qu'ils soumettent tous les 5 ans à la Commission un rapport sur l'application du paragraphe 2 en expliquant les raisons pour lesquelles ils estiment nécessaire de maintenir les catégories visées au paragraphe 2, point b, auxquelles ne s'applique pas le paragraphe 1er[225]. Il est intéressant de remarquer que cette obligation de motivation du maintien des exclusions ne s'applique donc qu'aux « *contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou des professions exerçant une autorité publique* »

Si une certaine liberté est donc ainsi conférée aux Etats membres, on s'aperçoit cependant que cet article reconnaît la qualité particulière des notaires et qu'on ne peut écarter trop rapidement l'hypothèse d'une conclusion de contrats immatériels en la forme authentique.

B. La problématique de l'acte authentique électronique

Nous nous proposons ici de nous interroger sur la compatibilité des nouvelles technologies avec l'authenticité. Plus qu'une esquisse, il s'agit ici de franchir le pas et d'envisager, de manière concrète, la réalisation d'actes électroniques à l'intervention des notaires. A cet effet, nous nous attacherons à dégager les principales objections et difficultés susceptibles de faire obstacle à la consécration d'un acte authentique électronique.

1. Objection d'ordre historique : prééminence de l'écrit-papier en matière d'acte authentique

La première objection qui vient à l'esprit lorsqu'on s'interroge sur l'acte authentique électronique est d'ordre historique, voire psychologique. Elle consiste à soutenir que

[225] D. GOBERT et E. MONTERO, "Le traitement des obstacles formels aux contrats en ligne", in *Le commerce électronique sur les rails ? Analyse et propositions de mise en œuvre de la directive sur le commerce électronique*, Cahiers du C.R.I.D., n° 19, Bruxelles, Bruylant, 2001, p. 204, n° 384.

l'authenticité est un mode de preuve littérale (section 1 du chapitre VI du Code civil) et qu'à ce titre le contrat authentique peut seulement revêtir la forme d'un écrit papier.

On sait que la preuve littérale n'a jamais été réellement définie par la loi, tant elle s'identifiait à l'écriture manuscrite apposée sur un support papier. De la même manière, l'acte authentique, et spécialement l'acte notarié a collé à cette image aujourd'hui désuète de la plume d'oie qui la traçait[226]. A l'heure actuelle cependant, force est de constater une évolution majeure, qui pour reprendre l'expression du Jeune Notariat français, marque le passage "de la plume d'oie à la plume-doigt"[227].

Le problème soulevé ici par les nouvelles technologies ne provient pas tant de la manifestation de la volonté d'une ou plusieurs parties à un acte que du mode probatoire de cet acte. Et ce problème surgit avec une acuité particulière s'agissant des actes authentiques.

"Si, après l'utilisation de support souples, tels le papyrus, le vélin, le parchemin, etc., celle du papier est aujourd'hui acquise, rien n'est définitivement figé et la réglementation peut facilement évoluer pour s'adapter aux nouvelles technologies. (…) Les changements techniques intervenus ces dernières décennies, qui ont introduit de nouveaux modes d'écriture dans la confection matérielle de l'acte notarié, comme la machine à écrire en 1923/1924, l'impression laser ou le recours au support télécopique un demi-siècle plus tard, n'ont pas nécessité de modifier la réglementation existante. En revanche, celle-ci n'est plus adaptée à l'apparition du contrat immatériel, ce qui ne signifie pas qu'elle est incompatible avec l'acte authentique (…)"[228].

Dès lors, si l'acte notarié est un mode de preuve incomparable et irremplaçable, le formalisme qui l'entoure ne doit pas autoriser un rejet de principe du contrat immatériel, au seul motif qu'il y a changement de support.

En outre, le recours à l'électronique décharge le notaire et ses collaborateurs d'une série de tâches administratives et leur permet de bénéficier d'une information plus rapide et plus complète. Mieux formés et informés, le notaire et ses collaborateurs disposent également de plus de temps pour conseiller leur clients, pour leur concocter des solutions "sur mesure".
C'est un rôle-clé pour le notaire, une véritable justice préventive. Cet aspect de la fonction notariale est souvent négligé, alors qu'il contribue à former un certain consensus social et, en évitant les procédures judiciaires longues et hasardeuses, permet de gagner en efficacité et de réaliser de substantielles économies. Envisagé sous cet angle, la numérisation contribue à renforcer la mission sociétale du notaire. Mais les nouvelles technologies de l'information et de la communication ne renforcent pas seulement le notaire dans son rôle social. Elles révolutionnent jusqu'à l'essence même de la fonction: à l'ère du papier succède l'ère de l'électronique.

2. Une difficulté d'ordre terminologique : La notion d'authentification

Une autre difficulté que l'on rencontre lorsque l'on parle d'acte authentique électronique est liée à la notion même d'authentification. Une telle difficulté est d'abord d'ordre

[226] G. ROUZET, "L'acte authentique à distance pour un aménagement du droit français de la preuve", in *Mélanges offerts à Roland de Valkeneer*, Bruxelles, Bruylant, 2000, p. 397.
[227] Jeune Notariat en action, *Le programme 2001-2002*, p. 3, disponible en ligne à l'adresse http :www.jeune-notariat.com/2001/mjn_programme.htm
[228] G. ROUZET, *op. cit.*, pp. 403-404.

terminologique. En effet, tant dans les textes de loi que dans la littérature relative aux problèmes juridiques posés par la transmission électronique d'informations, il est fréquent de recourir à la notion d'authentification.

A titre d'exemple, on peut voir qu'aux termes de l'article 2, 1 de la directive européenne du 13 décembre 1999, la signature électronique est appelée à servir de "méthode d'authentification".

Il y a lieu de dissiper les confusions autour de la notion d'authentification, surtout dans une matière telle que le droit de la preuve. Comme on a pu le voir, la loi ne définit pas l'authenticité ; elle se limite à préciser les conditions de son acquisition (article 1317 du Code civil). On peut donc préciser cette notion en se référant au sens usuel du mot.

Le terme authentique dans son acception usuelle désigne "ce dont l'origine ne peut être contestée", "ce qui est véridique".

Dans son Vocabulaire juridique, G. CORNU[229], donne du mot authentique la définition suivante :

"Authentique :

1. qui a véritablement l'auteur ou l'origine qu'on lui attribue ;
2. se dit plus techniquement, par opposition à l'acte sous seing privé, de l'acte qui, étant reçu ou parfois seulement dressé par un officier compétent, selon les formalités requises, fait foi par lui-même jusqu'à inscription de faux".

On constate que, de manière générale, le mot "authentique" se dit de ce qui est véridique, véritable, de ce à quoi on peut ajouter foi. Cependant, il prend deux acceptions, dont la distinction est utile pour notre propos.

Lorsque la majorité de la littérature juridique parle d'authentification, elle vise "en réalité l'authentification de la signature, dans la double fonction qui lui est traditionnellement reconnue: l'identification du signataire, et la manifestation de sa volonté de s'approprier le contenu du document qu'il signe. Et c'est pourquoi, lorsque cette signature est transmise par le moyen de l'électronique, il s'agira d'établir d'une part l'identité de l'émetteur du message, d'autre part l'intégrité du message lui-même. Le message sera 'authentifié' s'il répond à cette double condition"[230].

Cette terminologie ne nous semble pas adéquate lorsque l'on parle de signature électronique. En effet, l'authentification au sens de la loi organique sur le notariat recouvre une toute autre signification[231].

[229] G. CORNU, *Vocabulaire juridique*, Paris, P.U.F., 1987.

[230] J.-F. TAYMANS, "Recueillir et authentifier le consentement : l'expérience notariale confrontée à la certification électronique", *op. cit*, p. 349.

[231] Y. TIMMERMANS, "Signature électronique et certification : le notariat et les nouvelles technologies", in *Signature électronique et certification*, Actes du Colloque organisé à Louvain-la-Neuve, le 25 septembre 2001, pp. 2-3.

Il est utile de se référer brièvement à l'étymologie du mot "authentique"[232]. Celui-ci, dérivé du grec "authentikos", signifie: "ce qui a un auteur certain", et par conséquent, ce qui a de l'autorité et donc "dont le pouvoir est inattaquable".

Les actes de l'autorité publique ont par eux-mêmes le caractère d'authenticité, parce qu'ils sont ce qu'ils sont : actes de l'autorité publique. Et "c'est le propre des actes de l'autorité publique d'être authentiques"[233]. Il s'agit des actes du pouvoir législatif (lois, décrets,…), des actes du pouvoir exécutif (arrêtés royaux, ministériels…) et des autorités administratives (actes d'état civil, registre des conservateurs des hypothèques,…) et enfin des actes du pouvoir judiciaire (jugements et arrêts) et actes extrajudiciaires (huissiers de justice,…).

Dans le domaines des actes privés, les pouvoirs publics ont, par voie de délégation, conféré aux notaires le pouvoir de donner à leurs actes, selon les termes de la loi organique du notariat, *"le caractère d'authenticité attaché aux actes de l'autorité publique"* (article 1er de la loi de Ventôse). La source de l'authenticité de l'acte notarié réside donc dans la délégation donnée par les pouvoirs publics aux notaires à cette fin.

Naturellement, dans les actes qu'ils reçoivent, les notaires identifient des parties et certifient qu'elles ont eu la volonté de s'approprier le contenu de l'acte. Mais, l'authentification du consentement par le notaire va bien au-delà de cette double mission. En effet, l'authentification notariale porte non seulement sur la réalité de l'adhésion des parties à l'acte sur la base d'un consentement libre et éclairé, mais également sur le contenu de l'acte. Très différent est l'objectif de l' "authentification" électronique qui porte essentiellement sur la signature. On préférera alors avoir recours, en matière de signature électronique, au terme de "certification" - pour éviter un risque de confusion – qui atteste de la seule identité du signataire tout en accordant un label de sécurité à la transmission. En outre, il est important de remarquer que les prestataires de service certification n'authentifient jamais le contenu des conventions. "Cette circonstance, jointe à la qualité du tiers (officier public ou non), marque la différence essentielle entre l'authentification notariale et la certification électronique"[234].

Ainsi, la distinction qu'il y a lieu d'opérer entres les deux types d' "authentification" n'est pas seulement d'ordre terminologique, elle tient surtout à la nature même de l'authentification à laquelle il est procédé.

Cette distinction est d'ailleurs d'autant plus importante qu'à l'heure où l'on parle tantôt de notaire électronique (*cybernotary*), tantôt de tiers de confiance, certains s'interrogent sur une probable "balkanisation de l'authenticité"[235], voire s'inquiètent d'une "chute de l'acte authentique"[236]. Que faut-il en penser ?

Jusqu'ici, les notaires détenaient le (quasi-)monopole de l'authenticité. S'oriente-t-on dès lors vers un éclatement de la mission d'authentification ? Celle-ci serait partagée, demain, entre les notaires, d'une part, et une diversité d'autorités de certification plus que probablement d'obédience privée (appelées encore très significativement, tiers de confiance ou tiers

[232] H. CAPITANT, *Vocabulaire juridique*, Paris, P.U.F., 1930, v° Acte authentique.
[233] P. WATELET, *op. cit*, p. 23.
[234] D. GOBERT et E. MONTERO, "L'ouverture de la preuve littérale aux écrits sous forme électronique", *op. cit*., p. 123.
[235] *Ibidem*, p. 122.
[236] L. GRYNBAUM, "La loi du 13 mars 2000 : la consécration de l'écrit et de la preuve électronique au prix de la chute de l'acte authentique", *Communication – Commerce électronique*, 04/2000, n° 2/4, pp. 12-15.

certificateurs), d'autre part. A moins de penser qu'à terme, ces derniers se substituent purement et simplement aux premiers. Ou alors, il va-t-il, peut-être, falloir revoir à la fois la catégorie des officiers publics et la force probante particulière attachée à ce titre. En effet, qu'est-ce qui justifierait alors ce statut d'exception, au bénéfice des notaires, par rapport aux autres certificateurs ?

Pour beaucoup, l'intervention de ces nouvelles autorités de certification semblent sonner le glas de l'acte authentique. Avant de céder trop vite à toute forme de panique ou de résignation[237], il convient de mettre en évidence les spécificités de l'authentification notariale.

En réalité, comme il l'a été déjà souligné plus haut, "le régime d'authentification notariale est intimement lié à diverses garanties particulières qui, à ce jour, distinguent nettement cette dernière du service fourni par les autorités de certification". [238]

Cette distinction met en exergue la qualité particulière attachée à l'office des notaires dans les systèmes juridiques de droit latin. En effet, dans le cas du notaire, la fonction de conseil apparaît indissociable de sa fonction d'authentification. Le formalisme légal de l'acte authentique est guidé, fondamentalement, par un souci de protection du consentement des parties dès lors qu'elles s'apprêtent à contracter des engagements jugés importants, tels le mariage, l'achat-vente d'un bien immobilier ou la donation.

Le rôle du notaire est notamment d'assurer la qualité du consentement des parties et de certifier ce consentement. Il est aussi d'assurer la correction de l'acte, à tous points de vue, de manière à prévenir des litiges. Ce devoir relève de sa mission de confiance et de médiateur social. Un des aspects de son ministère légal est effectivement d'assurer le maintien de la paix sociale et d'empêcher la naissance de différends à propos d'actes privés. Aussi s'emploiera-t-il à écarter les clauses équivoques et susceptibles de donner lieu à une action en nullité ou en réscision, bref à vérifier la conformité de l'acte aux dispositions légales. A cet effet, il informera au mieux les parties sur les aspects juridiques de l'opération. Au-delà du renseignement *stricto sensu*, la mission de conseil du notaire le conduit à indiquer aux parties la voie la meilleure, parmi une diversité de solutions juridiques.

L'authentification notariale porte, en définitive, sur le contenu de l'acte et sur la réalité de l'adhésion des parties (identifiées) à celui-ci, sur la base d'un consentement libre et éclairé. Bien différente est l'authentification électronique qui porte seulement sur la signature. Nous renvoyons sur ce point à la partie consacrée à la certification (v. *supra*, chapitre I).

3. Les difficultés d'ordre pratique : la réception, la transmission et la conservation de l'acte authentique

Les objections pratiques à la consécration juridique de l'acte authentique électronique se situent à trois niveaux : celui de la réception de l'acte ; celui de la transmission de l'acte et

[237] Voir à ce sujet, les propos tragiques de L. GRYNBAUM (référence à la note précédante) sur le nouvel article 1317 du Code civil français…: "Un acte authentique dressé sur support électronique perdra toute sa force dès lors qu'il sera établi en dehors de la présence physique du notaire et des parties à l'acte. Le nouvel article 1317 en retirant le rôle de témoin privilégié à l'officier public prive l'acte authentique dressé sur support électronique de son essence et signe ainsi sa déchéance. En effet, il n'y aura, techniquement, pas de différence entre un acte authentique établi à distance et un acte sous seing privé dont les auteurs seront identifiés par des tiers."

[238] D. GOBERT et E. MONTERO, "L'ouverture de la preuve littérale aux écrits sous forme électronique", *op. cit.*, p. 122.

enfin celui de sa conservation. En effet, "la force probante de l'écrit dépendra des conditions dans lesquelles il aura été rédigé, conservé et éventuellement transmis"[239].

a) La réception de l'acte authentique

Comme on l'a déjà souligné, la réception par le notaire est l'élément fondamental de l'authenticité de l'acte notarié. Si la loi confère aux notaires le privilège de donner l'authenticité aux actes et conventions qu'ils reçoivent, ceux-ci doivent les recevoir moyennant le respect d'un certain nombre de formalités.

Parmi celles-ci on retiendra tout particulièrement la nécessité de la présence permanente du notaire auprès des parties.

Il semble en effet que la présence effective des notaires auprès de chaque partie soit une condition indispensable pour conférer l'authenticité à l'acte (v. *supra*, pt. II, c, 1) Il existe un rapport consubstantiel entre le processus d'authentification notariale et la présence physique de l'ensemble des parties[240]. Dès lors, si l'on admet que la singularité de l'acte authentique repose sur la présence réelle de l'officier au temps et au lieu de l'émission du consentement, il s'agit de rechercher si le formalisme qui conditionne cette authenticité demeure compatible avec le "contrat électronique", qui suppose une conclusion à distance.

Les solutions seront plus ou moins faciles à trouver, selon que l'acte doit se réaliser au sein d'un office notarial unique ou que l'on voudrait le conclure à distance [241]. C'est ce qui amène certains observateurs à établir une distinction, discutable s'il en est, entre acte authentique électronique et acte authentique conclu à distance.

Selon P. CATALA, dans l'hypothèse d'un acte réalisé au sein d'un office notarial unique, la rédaction de l'acte sur le clavier d'un ordinateur fait d'ores et déjà partie des mœurs et de la pratique professionnelle, grâce à l'usage des bases de données informatisées et du traitement de texte.

Ces procédures électroniques peuvent être entrecoupées d'éditions sur papier du texte, en cours d'élaboration et après achèvement. Le passage au papier *in fine* permet de recueillir les signatures et d'apposer le sceau du notaire selon le mode traditionnel. A partir de là, il est aisé de constituer parallèlement un minutier sur papier et son clone numérique[242]. Dans cette

---

[239] I. DE LAMBERTERIE, "L'écrit dans la société de l'information", in *Mélanges en l'honneur de Denis talon*, 1999, p. 128.

[240] P. GAUTIER et X. LINANT DE BELLEFONDS, "De l'écrit électronique et des signatures qui s'y attachent", *J.C.P.*, 2000, éd. E, n°31/34, p. 1275.

[241] P. CATALA, "Electronic signature", transl. by D. GUILD, disponible en ligne à l'adresse http://www.law.ed.ac.uk/legalconnexion/research/signelec.htm; P. CATALA, "Le formalisme et les nouvelles technologies", in *Journées Jacques Flour – Association Henri Capitant, Le formalisme, Répertoire Defrénois*, 2000, n°15/16, p.908, n°21 cité dans Union Internationale du Notariat Latin (CAUE), *Les nouvelles technologies informatiques et l'acte authentique*, Rapport de la Sous-Commission, sous pres. de Me G. ROUZET, Amsterdam, Fondation pour la promotion de la Science Notariale, 2001, pp. 4-7.

[242] Voir Extraits du discours de J.-L. MORIER (Prés. du 28ème Congrès du Mouvement Jeune Notariat), *Congrès 1997 : L'authenticité, la force*, Lisbonne, 8-12 octobre 1997, disponible en ligne à l'adresse http://www.jeune-notariat.com/pu_lisb.htm. Celui-ci évoque l'absurdité d'une telle pratique : "Les minutes restent sauvegardées dans l'ordinateur, alors qu'aujourd'hui nous rédigeons sur traitement de texte, nous tirons l'acte sur papier, nous archivons l'acte authentique sur place si l'espace le permet. Les notaires qui manquent de place microfilment les minutes qui sont posées plus loin et, dernier cri, des sociétés de services proposent de scannériser les minutes

perspective, où l'on combine les deux voies, il n'est même pas nécessaire de modifier les textes actuels.

Mais, on peut vouloir le "tout électronique", c'est-à-dire parfaire l'acte au clavier et à l'écran sans passer par le papier. Alors surgit le problème de la signature électronique qui ne se pose pas dans les mêmes termes pour le notaire et pour les parties.

S'agissant du notaire, il semble que le recours à la cryptographie puisse fournir une solution acceptable pour la signature comme pour le sceau. A nos yeux, cette double solennité, qui engage la foi de l'officier public en vers l'Etat, les parties et les tiers, est véritablement, au plan de la forme, l'âme de l'authenticité.

S'agissant des cocontractants , ainsi que des témoins instrumentaires, le cas échéant, plusieurs solutions sont envisageables.

La plus simple serait de recueillir leur signature en clair au clavier sous l'affirmation, par le notaire que les signataires ont eu pleine connaissance de l'acte et qu'ils ont exprimé et formalisé de la sorte leur consentement. Il n'est pas évident que l'on doive compliquer les choses en subordonnant à la cryptographie les signatures des parties et des témoins. En effet, la logique de l'acte authentique confère un rôle secondaire à la signature des parties. "A l'heure où il n'est question que de tiers certificateurs professionnels, qualifiés d'insoupçonnables, on doit reconnaître que l'officier ministériel, présent à l'acte qu'il reçoit, délégataire de la puissance publique, chargé par elle de vérifier le contenu des conventions, l'heure et le lieu, l'identité des parties et d'attester la réalité de leur consentement, celui qu'on appelle depuis toujours le témoin privilégié, est le tiers certificateur par excellence. On ne le connaissait pas sous ce nom parce que le vocable n'existait pas ; mais, dès avant qu'il en soit créé d'autres, le tiers certificateur existait d'ores et déjà en la personne des officiers publics"[243].

Au vu de ce qui précède, il semble dès lors possible, pour cette hypothèse (acte entièrement réalisé sous le signe de l'unité de lieu en l'office du notaire qui le reçoit), de recueillir sans bouleversement législatif majeur la version électronique de l'acte authentique.

L'hypothèse d'un acte authentique conclu à distance est, quant à elle, nettement plus problématique. Le contrat électronique se présente alors comme un contrat conclu à distance pour les parties, un "contrat entre absents". Le notaire peut-il, dans un tel contexte, conférer l'authenticité à la convention, alors qu'il ne saurait être simultanément placé aux deux extrémités de la chaîne en raison de la distance qui sépare les contractants de l'officier public ?[244]

A ce jour, les parties qui ne peuvent ou ne veulent se déplacer ont recours au mécanisme de la procuration ou du mandat. Ce mécanisme, admis par la plupart des législations européennes, existe déjà depuis un certain temps et ne semble pas poser de difficultés particulières. En effet, "cette pratique juridique justifie qu'il n'est pas besoin de recourir à un notaire unique et écarte l'objection qui voudrait que ce soit le même officier public qui recueille l'ensemble des

---

pour les archiver en CD-Rom… Ainsi la boucle est bouclée : la minute née de l'ordinateur, retourne dans l'ordinateur. Convenons que cela frise l'absurdité."

[243] P. CATALA, *op. cit.*, p. 6.

[244] G. ROUZET, *op. cit.*, p. 407.

consentements"[245]. Le consentement de la partie représentée a généralement été donné dans les jours précédents et dans un autre lieu que celui de la conclusion effective du contrat. Le notaire instrumentaire est alors différent de celui qui a reçu la procuration en la forme authentique. Ce mécanisme de procuration pourrait tout à fait continuer à s'appliquer mais sous une forme électronique[246].

Toutefois, si cette solution rejoint l'idée d'un acte notarié à distance, elle n'entend pas dispenser les parties et leur notaire respectif de se rencontrer. Elle ne consacre donc pas encore le "tout électronique". En effet, elle impose ici un contact physique entre chaque cocontractant et son notaire. L'officier public doit encore être présent auprès de chaque partie signataire pour instrumenter dans les conditions classiques afin de conseiller son client et de donner le caractère authentique à l'acte.

Pour J.-L. SNYERS[247], la dématérialisation complète de l'acte authentique ne serait pas une solution satisfaisante car elle méprise la condition primordiale de l'authenticité. Le contrôle du notaire en ressortirait très affaibli. En effet, le notaire contrôle si la personne qui se présente devant lui est bien celle qu'elle prétend être, il contrôle si le comparant comprend le contenu de la convention et l'éclaire à ce sujet. Le notaire contrôle également si le consentement du comparant est libre et éclairé. Selon cet auteur, ces contrôles deviendraient – par le recours aux technologies modernes – affaiblis, ce qui pour les actes de grande importance n'est pas opportun[248].

Cette solution intermédiaire de procuration semble être actuellement, aux yeux des officiers publics intéressés, la formule la plus adéquate. Ce qui pourrait donc s'avérer envisageable, c'est le recours à un mécanisme de procuration signée par transmission électronique[249]. Il convient seulement qu'un officier public soit présent auprès de chaque partie signataire pour instrumenter dans les conditions classiques. Ainsi faute d'avoir un notaire à compétence européenne[250], cela permettrait que des notaires compétents *ratione loci* soient placés à chaque extrémité du contrat et authentifient le contrat électronique chacun dans leur Etat d'origine, selon les règles qui y sont en vigueur.

En outre, la difficulté inhérente au concept d'acte à distance est encore renforcée par d'autres exigences qui s'imposent aux notaires, telles la connaissance des parties et la lecture de l'acte. Prenons l'exemple de la connaissance personnelle des parties. Il est nécessaire, en effet, que l'identité des parties ayant comparu devant le notaire soit établie avec certitude. Le notaire doit donc connaître les parties. L'exigence de la connaissance des parties par le notaire ne figure pas en termes explicites dans la loi de Ventôse.

---

[245] Union Internationale du Notariat Latin (CAUE), *op. cit*., p. 28.

[246] B. VUYLSTEKE, "Cybernotary", *Authenticité et Informatique*, Congrès des notaires (F.R.N.B.), Bruxelles, Kluwer – Bruylant, p. 465.

[247] J.-L. SNYERS, "De elektronische authentieke akte en de notariële, elektronische archivering", *Limb. Rechtsl*., 2000, p. 289.

[248] B. VUYLSTEKE, *op. cit.* p. 465. Mais le recours à des procédés tels que la de vidéoconférence ne semble cependant pas entièrement satisfaisant : "De hamvraag is natuurlijk of dit beantwoordt aan de authenticiteitsvereiste dat de notaris *de visu et auditu* vaststelt".

[249] J.-L. MORIER et S. GAILLARD-HOSTEIN, "L'authenticité dématérialisée", p. 12, disponible en ligne à l'adresse http://www.ugnf-snn.org/congres99/HTML/Authen_Dema.htm.

[250] Voy. à ce sujet, R. STÜRNER, "L'acte notarié dans le commerce électronique européen", *Rev. int. dr. comp*., 1996, pp. 516-532.

L'article 11 de la loi de Ventôse dispose seulement que : *"Le nom, l'état et la demeure des parties devront être connus du notaire, ou lui être attestés dans l'acte par deux personnes connues de lui, ayant les qualités requises pour être témoins instrumentaires".*

La *ratio legis* de cette disposition est d'empêcher tout risque de fraude par substitution de personnes ; elle tend à empêcher qu'une personne se fasse passer pour quelqu'un d'autre. Le notaire doit donc savoir pour chacun des comparants comment il se nomme (nom de famille), ce qu'il fait (état social), où il habite (habitation réelle). Pour cette raison, il faut considérer cette disposition comme étant d'ordre public. "Sans connaissance des parties le notaire, il n'est pas de certitude d'origine, et donc pas d'authenticité"[251].

Toutefois, force est de constater que la connaissance exigée dans le chef du notaire implique une connaissance personnelle des parties. Connaître quelqu'un, c'est pouvoir attester que la personne en cause est bien celle qu'elle prétend être. Cette connaissance du comparant, le notaire doit l'avoir personnellement lors de la réception de l'acte.

On sait cependant qu'une telle exigence de connaissance des comparants n'est plus réaliste à notre époque. En effet, les circonstances actuelles ne permettent plus de respecter le prescrit de l'article 11 ; celui-ci date d'un autre temps. Aujourd'hui, il n'est plus possible au notaire de connaître personnellement les parties ni de trouver dans son entourage des témoins qui les connaissent personnellement. Si ce phénomène n'est en soi pas propre aux nouvelles technologies, certains observateurs se demandent si ces dernières ne rendront pas les choses encore plus complexes[252]. Or, la contravention à l'article 11 donne lieu à la mise en cause de la responsabilité civile du notaire lorsque la substitution des personnes est prouvée…

Ces différentes difficultés n'ont apparemment pas empêché certains Etats européens de consacrer légalement l'acte authentique électronique. A cet égard, il est intéressant de se pencher sur les initiatives italienne et française.

L'Italie a été le premier Etat membre de l'Union européenne à légiférer en matière de signature électronique[253].

L'article 2703 du Code civil italien admet la technique de la signature par un notaire ou un autre officier public afin d'authentifier un acte. L'article 16 du Décret n°503 renforce cette nouvelle forme d'authentification par l'introduction de la signature digitale authentique (*firma digitale autenticata*). L'authenticité ainsi conférée est complète dans la mesure où le notaire aura pris le soin de constater que la signature digitale a été authentifiée en sa présence, et cela après avoir vérifié son identité ainsi que la validité de la clé publique et le fait que le document signé correspond à la volonté des parties et n'est pas en contravention avec l'ordre juridique au sens de l'article 18, § 1, 1° de la loi du 16 février 1913, n. 89. Ce décret impose au notaire, conformément au principe de base de l'authenticité notariale, d'effectuer un

[251] J. DEMBLON, *op. cit.*, t. XI, Livre VII, n° 192.

[252] Si d'un point de vue technique les choses peuvent paraître plus complexes, le certificat électronique, qui, rappelons-le, est généré par des autorités de certification qui auront pris le soin d'identifier les parties, ne peut-il pas aider le notaire dans cette tâche ?

[253] La loi n° 59/97 du 15 mars 1997, article 15, 2ème alinéa, en forme le socle, complété par les décrets du président de la République du 10 novembre 1997 et du président du Conseil des ministres du 8 février 1999.

contrôle strict du contenu de la convention. Il s'ensuit que la comparution personnelle devant le notaire reste obligatoire[254].

La loi française du 13 mars 2000 relative à la signature électronique consacre également l'existence de l'acte authentique électronique en ajoutant un nouveau paragraphe à l'article 1317 du Code civil. L'article 1317 du Code civil relatif à l'acte authentique dispose notamment qu' *"il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat"*. La dernière phrase du premier alinéa de l'article 1316-4 du Code civil ajoute : *"Quand elle (la signature) est apposée par un officier public, elle confère l'authenticité à l'acte"*.

Le législateur français a ainsi consacré le principe selon lequel l'acte authentique peut être dématérialisé et la signature de l'officier peut emprunter la forme électronique.

A première vue, la nouvelle loi ne modifie pas les conditions de validité de l'acte authentique, et notamment celle de la comparution du signataire auprès de l'officier public qui doit recueillir son consentement. En effet, l'article 1317 du Code civil, s'il consacre le principe de l'acte authentique électronique, ne propose aucunes règles concrètes relatives à son application.

Toutefois, étant donné la valeur attachée aux actes authentiques, la dématérialisation de ces derniers, tant sur un plan juridique que technique, exige une expertise approfondie de façon à ne pas remettre en cause les garanties de l'authenticité[255]. A cet effet, le texte légal renvoie prudemment la question de sa mise en œuvre pratique à un décret.

Enfin, les difficultés inhérentes à l'application pratique de l'acte authentique électronique, amènent certains observateurs à envisager des scénarios plus futuristes les uns que les autres. Ainsi, par exemple, a-t-il été suggéré de recourir aux techniques virtuelles, telles que la vidéoconférence[256]. Celle-ci pourrait même être couplée avec une procédure biométrique d'empreinte digitale. Toutefois, à l'heure actuelle, de telles technologies, si elles nous laissent entrevoir de formidables perspectives, ne nous paraissent encore être de l'ordre du possible, compte tenu notamment des coûts qu'elles sont susceptibles d'entraîner.

b) Le problème de la transmission de l'acte

Dès que l'on parle de "distance", se pose également le problème de l'échange et de la transmission mutuels des actes.

En effet, l'utilisateur doit pouvoir être assuré que le contrat qu'il visualise sur son écran, et qu'il veut signer électroniquement, est conforme au texte qui lui été envoyé et donc qu'il n'a pas été modifié dès le début ou en cours de transmission. Peut-on dès lors garantir l'intégrité du contenu d'un document numérique ?

---

[254] J.-L. SNYERS, "De elektronische authentieke akte en de notariële, elektronische archivering", *op. cit.*, p. 287.
[255] H. ROBERT, *La preuve dans les télécommunications*, (Me Breban sous dir. de), DESS Droit du Numérique et des nouvelles techniques, 1999-2000, p. 39, disponible en ligne à l'adresse http://www.ifrance.com/droitntic/Memoire_Robert.htm?.
[256] V. WEYTS, "A room with a view : van de klassieke naar de elektronische nataris", *Jur. Falc.*, n°33, 1996-1997, p. 73.

"Dans un système basé sur du papier, le message est fixé sur un support d'information matériel. Dans un tel environnement , il est aisé de vérifier l'intégrité du document : primo, parce que toute manipulation du document laisse des traces et secundo, parce que le *Code Napoléon* impose que les actes juridiques soient constatés dans autant de supports d'information papier qu'il y a de parties. Un message électronique, en revanche, est expédié comme un flux d'électrons qui ne laisse au cours du transfert aucune trace sur les moyens de transmission."[257]

Si un tel "flux d'électrons" offre des incontestables avantages de rapidité et de précision, son inconvénient majeur semble résider dans le caractère transitoire et vulnérable des transactions qu'il permet de mettre en œuvre.

On sait notamment à quel point les supports numériques peuvent tantôt faire l'objet de manipulations par des *hackers*, tantôt être contaminés par des virus.[258]

En outre, il n'est pas inutile de souligner que dans les environnements numériques, l'intégrité ne doit pas seulement concerner les données contenues dans le message, mais également le message lui-même. En effet, les environnements numériques ne permettent pas de distinguer l'original des copies. "Aussi, une sécurité supplémentaire doit-elle être prévue au moyen d'un contrôle sur le flux des messages : chaque message (…) doit nécessairement comporter un numéro d'identification séquentiel unique, lequel doit, bien entendu, être protégé soigneusement par la mécanisme qui protège l'intégrité globale des données"[259].

Les difficultés relatives à l'intégrité des données sont principalement tributaires des moyens technologiques. Celles-ci ne pourront être résolues que moyennant un recours adéquat à des procédures techniques de sécurisation.

c) Conservation et archivage de l'acte authentique

L'obligation de conservation des archives a pour objet d'instituer un mécanisme de garanties de pérennité de la preuve des actes authentiques. "On peut dire , sans risque de se tromper, que la valeur de l'acte authentique des notaires réside pour une large part, dans la sécurité de conservation de l'instrument de preuve (…)"[260].

Le devoir de conservation du notaire est principalement imposé par les articles 1er, 20 et 22 de la loi de Ventôse.

Article 20 :

"*Les notaires sont tenus de garder minute de tous les actes qu'ils recevront.(…)*"

---

[257] W. WILMS, "De la signature au 'notaire électronique'. La validation de la communication électronique", *Mélanges Jean Pardon*, Bruxelles, Bruylant, 1996, p. 568. Contra, Union International du Notariat Latin, *op. cit.*, p. 26 :"La fluidité de l'écrit électronique n'est pas en soi une cause inéluctable de fragilisation du document matérialisé et si la numérisation présente un risque d'interception ou de dénaturation qui n'est pas propre au document électronique, il reste cependant indépendant du support. Le danger – non négligeable – de fragilité de l'écrit numérique demeure, semble-t-il, comparable à celui de l'écrit rédigé à l'encre sur un support papier."

[258] V. WEYTS, *op. cit.*, p. 68.

[259] W. WILMS, *op. cit.*, p. 568.

[260] P. HARMEL, *Organisation du notariat et déontologie du notariat*, Livre II, Notes de cours, 1973-1974, p. 112, n° 115.

Article 22 :

"Les notaires ne pourront se dessaisir d'aucune minute si ce n'est dans les cas prévus par la loi ou en vertu d'un jugement.(…)"

Article 23 :

"*Les notaires ne pourront également, sans l'ordonnance du président du tribunal de première instance, délivrer d'expédition ni donner connaissance des actes à d'autres qu'aux personnes intéressées en nom direct, héritiers ou ayants droit, à peine de dommage-intérêts, d'une amende de 100 francs, et d'être, en cas de récidive, suspendus de leurs fonctions pendant trois mois ; sauf néanmoins l'exécution des lois et règlements sur le droits d'enregistrement, et de celles relatives aux actes qui doivent être publiés dans les tribunaux*."

Les archives notariales appartiennent au domaine public[261]. A ce titre, les archives sont inaliénables, imprescriptibles et non susceptibles d'appropriation privée.

Le devoir de conservation s'applique à l'ensemble du "protocole notarial", c'est-à-dire aux minutes et documents y annexés, aux répertoires ainsi qu'aux actes déposés ou rapportés pour minute[262]. Les actes authentiques doivent être conservés pendant une très longue période. Le notaire lui-même est amené à conserver les actes de 50 à 75 ans. Après cela, les archives royales continueront de les archiver.

Le devoir de conservation qui incombe ainsi au notaire entraîne deux obligations :

- le dépôt doit être conservé chez le notaire, c'est-à-dire au siège de son étude ;
- le dépôt doit être protégé autant que faire se peut de la destruction et du vol.

L'utilisation des nouvelles technologies en matière d'archivage soulève plusieurs difficultés[263]. Le problème de la confidentialité inhérente à la conservation notariale mérite qu'on s'y attarde quelque peu. En effet, traditionnellement, l'avantage de la conservation d'un acte chez le notaire est la garantie de la confidentialité. Le déposant doit en effet pouvoir disposer de toutes les garanties que le document est couvert par le secret professionnel du notaire, et qu'à ce titre, il ne sera pas communiqué à des tiers.

Les restrictions apportées à la communication des actes prévues par l'article 23 de la loi de Ventôse procèdent de leur obligation générale de secret professionnel (article 458 du Code pénal). "Ce devoir de conserver comme secret, tout acte vis-à-vis des autres personnes, participe-t-il à l'obligation de secret ? Il en dérive, comme une application, et jusqu'à un certain point une extension puisque le droit de communication est restreint, même si, par nature, l'acte n'était pas secret. L'article 23 crée, à nos yeux, une présomption légale de secret"[264]. On voit à quel point l'obligation de conservation du notaire est intimement liée au principe du secret professionnel et de la confidentialité.

---

[261] R. DE VALKENEER, *op. cit*, p. 106, n° 181.
[262] P. HARMEL et R. BOURSEAU, *Les sources et la nature de la responsabilité civile des notaires, 1830-1962*, La Haye, Faculté de droit de Liège et M. Nijhoff, 1964, p. 103.
[263] E. MONTERO et A. WALLEMACQ, "La responsabilité du notaire comme auteur, récepteur ou utilisateur du document informatique", in *Authenticité et Informatique*, Congrès des notaires (F.R.N.B.), Kluwer- Bruylant, 2000, pp. 425-450, spéc. pp. 429-430.
[264] P. HARMEL, *op. cit.*, p. 139, n° 145.

A l'heure actuelle, plusieurs observateurs ont fait allusion à la possibilité pour les notaires de confier la conservation de leur archives à des entreprises d'archivage qui seraient de nature privée. Une telle délégation de leur fonction de conservation semblerait en effet offrir de nombreux avantages, tant sur le plan logistique (compétence technique) que sur le plan économique (coûts). Dans un tel contexte, peut-on envisager que celui-ci délègue ainsi sa fonction de conservation ? Pour certains, cette solution paraît impensable dans la mesure où ils contestent formellement qu'une entreprise commerciale d'archivage puisse offrir la moindre garantie de confidentialité[265].

Une position aussi radicale doit, selon nous, être remise en question. En effet, la voie conventionnelle permettrait d'offrir des possibilités. Il est tout à fait concevable pour les notaires de confier la conservation de leurs actes à des entreprises privées – certainement plus aptes à faire face aux difficultés techniques – moyennant l'imposition dans le contrat d'une clause de confidentialité. L'objection nous paraît être plus de nature psychologique que juridique. Le notariat semble en effet redouter de sacrifier son indépendance dans la mesure où il sera amené à dépendre des techniciens informatiques pour conserver ses archives et les utiliser.

Toutefois, à titre d'exemple, il est intéressant de noter que le notariat autrichien a mis en œuvre un système d'archivage central électronique. Cette initiative est organisée à l'échelon national avec l'appui d'une multinationale, la société Siemens. Le système mis en place fonctionne selon un structure mixte. Chaque office notarial doit déposer les actes notariés établis depuis le 1er janvier 2000 à ces archives électroniques (dénommées *CyberDOC*). "En pratique, l'acte tiré sur papier puis 'scannérisé' avant d'être archivé électroniquement, mais il ne semble pas que cette formalité évite l'utilisation du support papier ou remplace l'établissement d'un original"[266].

Enfin, dans la matière du droit de la preuve, la conservation des documents est un élément fondamental puisqu'ils sont susceptibles d'être utilisés ultérieurement. Cette conservation doit donc être opérée de manière fiable. Cet élément soulève cette fois une difficulté d'ordre technique relative à la qualité de conservation des documents, qui dépasse le cadre de la présente étude.

Il est d'usage de caractériser le document par trois qualités fonctionnelles qui déterminent la valeur dudit document : l'intégrité, la lisibilité et la stabilité. S'agissant de l'acte authentique, et de sa conservation par voie électronique, il apparaît qu'une qualité maximale de conservation devra être requise.

Concernant les difficultés d'ordre général inhérentes à la pratique de l'archivage électronique, nous renvoyons sur ce point à la partie générale relative à la conservation et l'archivage (v. *supra*, chapitre II).

---

[265] J.-L, SNYERS, "De elektronische authentieke akte en de notariële, elektronische archivering, *op. cit.*, p. 303.

[266] Union Internationale du Notariat Latin (CAUE), *op. cit.*, pp 17 s. Voy. à ce sujet, les réflexions du Jeune Notariat français, *op. cit.*, p. 5 ; il apparaît utile d'établir une distinction entre le moment de la passation de l'acte et le temps de conservation de celui-ci. Pour les minutes numériques, il semble nécessaire que l'officier public ait la possibilité de créer un deuxième original papier, sous sa seule signature manuscrite, original qui sera conservé classiquement et permettra la délivrance des copies authentiques ou exécutoires papier. Ainsi l'éthique d'indépendance à l'égard des fournisseurs techniques sera préservée, sans rejeter la technologie elle-même, s'agissant de la passation de l'acte.

IV. RÉFLEXIONS FINALES ET RECOMMANDATIONS

A. Il a été souligné ci-dessus qu'il y a lieu d'opérer une distinction fondamentale entre deux types d' "authentification" : celle réalisée par les autorités de certification et celle inhérente à la fonction notariale. Un telle distinction n'est pas seulement d'ordre terminologique, elle tient aussi et surtout à la nature même de l'authentification à laquelle il est procédé.

Cependant, la situation pourrait évoluer. Les tiers certificateurs pourraient voir leurs fonctions s'élargir, de telle sorte que, pour certains, leur mission spécifique s'apparenterait alors réellement à celle des officiers publics. "L'on pourrait également imaginer d'étendre la mission de ce tiers à la conservation des documents informatiques, à la délivrance du certificat d'envoi et de réception de ce document et à l'absence d'altération durant cette transmission"[267]. Faudra-t-il alors y voir un éclatement de la mission d'authentification, une "chute de l'acte authentique"[268]. Une telle conclusion nous paraît hâtive. En effet, si une telle hypothèse aura pour conséquence de modifier certaines choses, d'une part elle n'est pas à envisager dans l'immédiat, d'autre part elle ne modifiera pas l'essence même de la mission légale du notaire : authentifier l'acte et conseiller les parties.

Cependant, il est certain que cette hypothèse appelle non seulement un changement de mentalités mais surtout une prise de position de la part du notariat, tant sur le plan national qu'européen. Celui-ci, par exemple, pourrait envisager d'investir lui-même le champ de l'enregistrement, voire de la certification[269]. En outre, des formes de collaboration pourraient s'instaurer entre tiers certificateurs, garants de la sécurité technique, et notaires, garants de la sécurité juridique. S'agissant, par exemple, de la comparution personnelle des parties devant le notaire, on a vu qu'il fallait distinguer selon que l'acte est dressé dans un office notarial unique ou qu'il est conclu à distance.

Dans la première hypothèse, il apparaît que tant que le titre ne quitte pas l'étude du notaire rédacteur, il n'est besoin d'aucun autre certificateur que l'officier public lui-même. Celui-ci est alors le tiers de confiance par excellence. "Il en va autrement et l'interposition d'un tiers devient nécessaire, lorsque le titre circule : c'est le prix du déplacement"[270]. Il faut en effet garantir à ce déplacement une sécurité maximale pour qu'aucun doute ne puisse planer sur la fiabilité de l'acte authentique. Dans ce contexte, l'intervention d'un tiers certificateur du meilleur niveau nous semble devoir s'imposer sur la trajectoire du document électronique.

B. Les caractéristiques des nouvelles technologies remettent en cause l'image, déjà largement brouillée pour certains[271], d'une authenticité notariale, dépendante d'un ensemble de règles de forme nombreuses, strictes, et finalement peu adaptées aux nécessités de la vie actuelle.

---

[267] P. VAN DEN EYNDE, "Conclusion : L'avenir de l'acte authentique : vers un nouveau support", in *Authenticité et Informatique*, Congrès de Bruxelles, F.R.N.B., Bruxelles, Bruylant, 2000, p. 493.

[268] L. GRYNBAUM, "La loi du 13 mars 2000 : la consécration de l'écrit et de la preuve électronique au prix de la chute de l'acte authentique", *Communication – Commerce électronique*, 04/2000, n° 2/4, pp. 12-15.

[269] C. PISANI, "L'acte dématérialisé", *Arch. Philos. Dr.*, t. 43, Le droit et l'immatériel, p. 159.

[270] P. CATALA, "Le formalisme et les nouvelles technologies", in *Journées Jacques Flour – Association Henri Capitant, Le formalisme, Répertoire Defrénois*, 2000, n°15/16, p.908, n°21 cité in Union Internationale du Notariat Latin (CAUE), *op. cit.*, p. 7.

[271] M. HANOTIAU, "Vers une autre authentification", in *Société, Notariat, Université*, Actes du colloque du 14 mars 1986, Louvain la-Neuve, Cabay-Bruylant, 1986, pp. 146-161, spéc. pp. 158-159. "Ces règles ont-elles encore une raison d'être ? L'on peut en douter. Elles finissent en fait par perdre tout sens et par devenir de

Au-delà des critiques que l'on peut formuler à l'encontre du "formalisme notarial", nul ne peut contester que les nouvelles technologies requièrent que soit réévaluée la nécessité de chacune des solennités légalement exigées pour qu'un acte soit authentique.

Parmi celles-ci, on sait que la présence physique et simultanée des parties et du notaire en son étude ainsi que ses corollaires (obligation de procéder à la lecture et au commentaire des mentions essentielles à l'acte, ainsi que la connaissance personnelle des parties) pose problème. A cet égard, il s'agit d'analyser si de telles exigences sont inhérentes à la fonction d'authentification et s'il est concevable d'en substituer un équivalent fonctionnel.

Pour certains, ce serait un recul de vouloir se passer, pour certains actes graves (mariage, vente d'un immeuble), de l'acte notarié en présence physique des parties et du notaire. Mais on imagine que, pour d'autres types d'actes, le notaire puisse s'acquitter à distance, par un biais électronique, des devoirs dont il est investi.

En outre, on constate également que certaines dispositions imposent l'utilisation du support "papier". A titre d'exemple, certaines règles fiscales prévoient des obligations relatives à l'utilisation du papier timbré ou encore l'utilisation d'un cachet[272].

Un nouveau formalisme devra être envisagé, qui prenne acte des spécificités de l'environnement numérique. Ce bref aparté sur la nécessité de repenser le formalisme entraîne une autre question : est-il concevable de prévoir un régime juridique unique, applicable à l'ensemble des actes authentiques ? A cet égard, nous renvoyons aux recommandations du chapitre II de la présente étude. Il semble en effet, que sur un plan législatif, il serait opportun de combiner deux approches, en adoptant une disposition transversale consacrant l'acte authentique électronique, tout en prévoyant une délégation au Roi pour opérer des modifications spécifiques à mesure que serait relevé un obstacle à la réalisation, la transmission et la conservation d'actes authentiques sous forme électronique.

C. A l'instar de nos voisins français, il serait donc opportun, pour une première étape, que le législateur belge consacre l'acte authentique électronique. La Fédération du notariat plaide d'ailleurs "vigoureusement auprès des autorités publiques pour que soient reconnues l'existence et, surtout, la valeur légale de l'acte authentique électronique (…)[273]"

La France, en effet, n'a pas traîné dans l'adoption d'une législation sur la preuve électronique. Le 13 mars 2000, elle adoptait la loi n°2000-230 "portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique"[274].

L'article 1317 du Code civil français y consacre l'acte authentique électronique. Cet article spécifique à l'acte authentique dispose en effet que celui-ci *"peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixés par décret en Conseil d'Etat.*"

---

véritables hypocrisies, tout en constituant nécessairement un frein pour un recours plus rapide et spontané à la forme authentique. Leur suppression pure et simple ne remettrait pas en cause la sécurité des actes notariés".

[272] J.-L. SNYERS, "De notariële certificatie en de elktronische authentieke akte", *op. cit*., p. 399.

[273] Fédération royale du Notariat belge, *Rapport annuel 2000 – Le notariat et les nouvelles technologies*, p. 2, disponible en ligne à l'adresse http://www.notaire.be/info/rapport_annuel_2000.htm.

[274] Loi n° 200-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, *J.O*., n° 62 du 14 mars 2000, p. 3968.

L'article 1316-4, alinéa 1er ajoute en outre : *"Quand elle [la signature] est apposée par un officier public, elle confère l'authenticité à l'acte.*"

Par ces articles, le législateur a voulu poser d'ores et déjà le principe que l'acte authentique peut être dématérialisé et que la signature de l'officier public peut emprunter la forme électronique. Toutefois, étant donné l'importance de pareil acte et la volonté de veiller à ce que sa dématérialisation ne remette pas en cause les garanties d'authenticité, la France veut se donner le temps d'effectuer un travail d'approfondissement tant sur le plan juridique que technique en vue de vérifier que les exigences d'authenticité peuvent être préservées dans un environnement dématérialisé. C'est pourquoi le texte renvoie sagement la question de sa mise en œuvre pratique à un décret.

Une première approche transversale – inspirée de celle qui a été adoptée par la loi française pour l'acte authentique électronique – semblerait donc envisageable. La Belgique pourrait faire de même via un arrêté royal, pourvu qu'une loi préalable consacre la possibilité de l'acte authentique électronique. Une telle loi préalable pourrait bien être celle relative à certains aspects juridiques des services de la société de l'information, en cours de préparation sous l'égide du Ministère des Affaires économiques. A cet égard, dans le prolongement d'une étude réalisée pour ledit Ministère visant à transposer la directive du 8 juin 2000 sur le commerce électronique, les auteurs avancent une première proposition d'avant-projet de loi[275].

Nous partageons les vues des auteurs de cette étude concernant leur modification de l'article 1317 du Code civil. Au chapitre VIII (dispositions finales) de cette proposition, les auteurs suggèrent en effet de compléter l'article 1317 de notre Code civil de la manière suivante :

"*Il peut être dressé sur tout support s'il est établi et conservé dans des conditions fixées par le Roi, par arrêté délibéré en Conseil des ministres*".

Parallèlement à cette modification législative d'ordre général, il nous semble également opportun de procéder, spécialement en ce qui concerne les actes notariés, à une modification de l'article 13 de la loi de Ventôse.

L'article 13 de la loi de Ventôse dispose en effet que :

"*Sans préjudice des prescriptions des articles 971 à 988 et 1001 du Code civil, relatifs aux testaments, les actes des notaires seront écrits à la main ou établis par des procédés mécaniques, tels la dactylographie, l'imprimerie, la lithographie, la typographie, d'une manière indélébile, lisiblement (…)*

Le Roi peut prescrire les mesures propres à assurer la conservation en bon état des actes notariés, pour la rédaction desquels il est fait usage de procédés mécaniques."

On s'aperçoit en effet que si cette disposition ne fait pas expressément référence au support "papier", elle y fait allusion de manière implicite. Si le terme "mécanique" rime avec

[275]Voy., la proposition de modification législative en annexe au *Commerce électronique européen sur les rails ? Analyse et propositions de mise en œuvre de la directive sur le commerce électronique*, Cahiers du C.R.I.D., n° 19, Bruxelles, Bruylant, 2001, pp. 403-429.

"électronique", il ne recouvre pas la même notion[276]. Il convient dès lors de procéder à l'actualisation de cet article.

Ces recommandations de modifications législatives, si elles constituent une avancée substantielle vers la consécration de l'acte authentique électronique, n'en sont cependant qu'une première étape. Il ressort en effet de la présente étude que la problématique de "l'acte authentique électronique" est d'une grande amplitude, en raison de la diversité tant des actes qu'elle concerne que des difficultés qu'elle fait apparaître (authentification, formalisme, transmission, conservation…).

Dès lors, dans le prolongement du présent rapport intermédiaire et suite aux débats et réactions que nos recommandations susciteront, ces questions devront être approfondies et étudiées notamment à la lumière des futures concertations avec les milieux concernés.

[276] J.-L. SNYERS, "De notariële certificatie en de elektronische authentieke akte", *Authenticité et Informatique*, Congrès des notaires, Bruxelles, Kluwer – Bruylant, 2000, p. 399 : "Elektronika en mechanica zijn geen synoniemen voor hetzelfde begrip"