L'encadrement juridique de "Documents Transférables Électroniques"

Nabil Gamal Eldine

THÈSE

Pour obtenir le grade de

Docteur

Délivré par **l'Université de Montpellier**

Préparée au sein de l'école doctorale
Droit et Sciences politique
Et de l'unité de recherche laboratoire de droit privé

Spécialité : Droit privé et sciences criminelles

Présentée par **Mr. Nabil GAMAL ELDINE**

L'ENCADREMENT JURIDIQUE DE 'DOCUMENTS TRANSFÉRABLES ÉLECTRONIQUES'

Soutenue le 19 janvier 2017 devant le jury composé de

Madame Elisabeth TARDIEU-GUIGUES	Maître de Conférence HDR, Faculté de droit de Montpellier	Directrice de Thèse
Madame Nathalie MALLET POUJOL	Directrice de recherche CNRS Montpellier	Présidente du jury
Monsieur Yvan AUGUET	Professeur à l'université de Perpignan	Rapporteur
Madame Alexandra MENDOZA-CAMINADE	Maitre de conférences HDR à l'université de Toulouse Capitole	Rapporteur

« La faculté n'entend donner aucune approbation aux opinions émises dans cette thèse ; ces opinions doivent être considérées comme propres à leur auteur ».

REMERCIEMENTS

Je tiens à remercier, tout d'abord, Madame le Professeur TARDIEU-GUIGUES Élisabeth, de m'avoir acceptée en tant que doctorant sous sa direction pendant ces cinq dernières années, sa disponibilité, ses relectures attentives et ses précieux conseils pour conclure ce travail.

J'adresse également mes remerciements à mes parents pour leur amour inestimable, leur confiance, leur soutien, leurs sacrifices et toutes les valeurs qu'ils ont su m'inculquer. Je remercie aussi mon frère Hossam GAMAL pour toute l'affection qu'il m'a donnée et pour ses précieux encouragements.

Je remercie enfin, tous mes amis qui m'ont soutenu durant ces cinq dernières années pour accomplir ce travail.

L’ENCADREMENT JURIDIQUE DE ‘DOCUMENTS TRANSFÉRABLES ÉLECTRONIQUES’

SOMMAIRE

ABRÉVIATIONS

Adde.	Ajouter
al.	alinéa
AAI	Autorité administrative indépendante
AC	Autorité de certification
A.E.	Autorité d'enregistrement
ANSSI	Agence National de la Sécurité des Systèmes d'Information
Art.	article
CA	Cour d'appel
Cass	Cour de cassation
CCI	Chambre de Commerce Internationale
CEDH	Convention européenne des droits de l'homme
CNIL	Commission nationale de l'informatique et des libertés
Rev.	Revue
Chrono	Chronique
CJCE	Cour de justice des Communautés européennes
CJUE	Cour de justice de l'Union européenne
CNUDCI	Commission des Nations unies pour le droit du commerce

	International
Coll.	Collection
Convention LU	Convention de Genève portant loi uniforme
Comm. com. électr.	Communication, commerce électronique
CD	*Compact Disc*
CERN	Centre Européen de Recherche Nucléaire
CSPN	Certification de Sécurité de Premier Niveau
D.	*Recueil Dalloz*
DDHC	Déclaration des Droits de l'Homme et du Citoyen
DMCA	*Digital Millennium Copyright Act*
DOI	*Digital Object Identifier* (en français : Identifiant d'objet numérique)
DRM	*Digital Rights Management* (en français : Gestion des droits numériques)
DVD	*Digital Versatile Disc*
EAL	*Evaluation Assurance Level*
eIDAS	Règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance

Éd.	Édition, Éditeur
EDI	Échange de données informatisé
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
ENST	École Nationale Supérieure des Télécommunications
EUCD	European Union Copyright Directive Directive
FAI	Fournisseur d'accès à Internet
Gaz. Pal.	Gazette du Palais
GED	Gestion électronique de documents
GRATE	*Global Access to Emulation Services*
IaaS	*Infrastructure as a service*
Ibid	le même auteur
IGC	Infrastructure de gestion des clés
Infra	infra ci-dessous
IP	Internet Protocol
ISO	Organisation internationale de normalisation
JCP	Semaine juridique
JDI	Journal du droit international
JOCE	Journal officiel des Communautés européennes
QPC	Question Prioritaire de Constitutionnalité
LCEN	Loi pour la confiance dans l'économie

	numérique
NIST	*National Institute of Standards Technology*
NTIC	Nouvelles technologies de l'information et de la communication
CPC	Code de procédure civile
ODF	*Open Document Format*
OS	Système d'exploitation
P.A.	Petites affiches
PaaS	*Platform as a service*
PDF	*Portable Document Format*
PME	Petites et moyennes entreprises
PSC	Prestataires de services de confiance
PSHE	Prestataires de services d'horodatage électronique
KEEP	*Keeping Emulation Environment Portable*
RCDIP	Revue critique de droit international privé
RDAI	Revue de droit des affaires internationales
RGAA	Référentiel général d'accessibilité des administrations
RGI	Référentiel général d'interopérabilité
RGS	Référentiel général de sécurité

RTD.civ.	Revue trimestrielle de droit civil
RPV	Réseau Privé Virtuel
Rev. trim. dr. Com	Revue trimestrielle de droit commercial
SaaS	*software as a service*
SSO	*Single Sign-on*
TCP	*Transmission Control Protocol*
TGI	TGI Tribunal de grande instance
TLC	Technologies de l'information et de la communication
TPE	Très petites entreprises
UCC	Uniform Commercial Code
URL	*URL Uniform resource locator*
vol.	*volume*
WWW	*World Wide Web*

INTRODUCTION

1. Le développement des nouvelles technologies constitue un progrès indéniable et a porté une influence remarquable sur l'exercice des activités bancaires et financières. Au fil des années, les NTIC (nouvelles technologies de l'information et de la communication) ont apporté des modifications majeures aux métiers de la finance[1]. Ces nouvelles technologies continuent à transformer les métiers traditionnels des établissements de crédit et des entreprises d'investissement[2], et donc les relations de ces prestataires financiers avec leurs clients. Désormais, ces relations peuvent se créer et s'entretenir à distance et de façon quasi-instantanée ce qui les distingue par leur nature des relations devant un guichet de banque ou par courrier. Contribuant à cette évolution, l'émergence d'un nouveau support pour les transactions bancaires et financières : le réseau Internet[3].

2. Avec Internet, nous passons à l'ère du commerce électronique, aujourd'hui considéré comme indispensable à la vie moderne. Nous utilisons l'internet pour accomplir des taches qui relèvent de notre vie quotidienne, comme par exemple faire ses courses en ligne ou encore les opérations bancaires effectuées en ligne (virement, consultation de solde…etc.) C'est un fait indéniable, Internet fait aujourd'hui partie intégrante de notre quotidien. Aussi, plutôt que de rechercher des moyens de ralentir le progrès technologique, vu par certains comme une cause de l'insécurité sociale, il convient de reconnaitre l'importance d'Internet dans le quotidien des usagers et d'établir des moyens de protection de leur vie privée.

---

[1] V. Les métiers financiers face à Internet : *Rev. éco. fin.* 2003, n° 69.

[2] B. Sousi, L'adaptation du droit bancaire et financier européen aux nouvelles technologies : *RJ com.* 2001, p. 77 ; La banque électronique : CNCT août 1997. – V. aussi, H. Spiteki, Banque universelle et technologies, perspectives et enjeux : *Rev. éco. fin*. 1995, n° 32 ; Vers la Banque de l'an 2000 : Banque Magazine janv. 1999.

[3] C. Féral-Schuhl, Les apports du droit de l'informatique et des nouvelles technologies, dix risques à anticiper dans les contrats : Dr. et patrimoine 3/2003, p. 59. – P. Catala, Le formalisme et les nouvelles technologies : Defrénois 2000, art. 37210, p. 897.

3. En raison de l'évolution spectaculaire des NTIC, le commerce électronique se situe dans une phase beaucoup plus mature qu'auparavant, notamment après l'expérience couronnée de succès de l'utilisation de la signature électronique. L'heure est au dépassement des frontières étatiques et à l'émergence d'une nouvelle ère dématérialisée où le commerce international doit composer avec Internet.

4. En France, pour régulariser l'univers informatique et promouvoir la communication électronique, la grande loi de l'internet a été mise en œuvre ; il s'agit de la loi du 21 juin 2004 sur la confiance dans l'économie numérique, dite LCEN[4] qui envisage les contrats électroniques comme prenant place dans le commerce électronique[5]. L'article 14 de ladite loi prévoit que :

« *Le commerce électronique est l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services.*

Entrent également dans le champ du commerce électronique les services tels que ceux consistant à fournir des informations en ligne, des communications commerciales et des outils de recherche, d'accès et de récupération de données, d'accès à un réseau de communication ou d'hébergement d'informations, y compris lorsqu'ils ne sont pas rémunérés par ceux qui les reçoivent.

Une personne est regardée comme étant établie en France au sens du présent chapitre lorsqu'elle s'y est installée d'une manière stable et durable pour exercer effectivement son activité, quel que soit, s'agissant d'une personne morale, le lieu d'implantation de son siège social ».

[4] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, version consolidée au 09 novembre 2016, [En ligne : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=id].

[5] V. notamment X. Linant de Bellefonds, *De la LSI à la LCEN ; C. Caron, Aspects de propriété intellectuelle* ; J.-M. Coblence, *Le statut de la publicité ;* Ph. Stoffel-Munck, *La réforme des contrats du commerce électronique ;* O. Cachard, *Définition du commerce électronique et loi applicable : Comm. comm. électr. 2004)*

5. A cet article 14, s'ajoute le texte de l'article 16 de la LCEN[6] qui détermine les limites au champ d'application de la loi et à l'harmonisation qu'elle opère. Ces exclusions relèvent de certaines opérations et modes d'activité, principalement pour des raisons d'ordre politique, telles que les jeux d'argent, la représentation en justice ou encore l'activité de notaire[7].

6. Au niveau européen et communautaire, il faut admettre que toutes les prestations réalisées matériellement ne peuvent pas être transposées dans l'univers électronique. La directive du 8 juin 2000[8] portant sur "*certains aspects juridiques"* du commerce électronique l'a bien précisé, dans son considérant n°18 ; elle prévoit qu'il y a "*des activités qui, de par leur nature, ne peuvent pas être réalisées à distance ou par voie électronique, tel que le contrôle légal des comptes d'une société ou la consultation médicale requérant un examen physique du patient*". Ainsi, nous réalisons que tout ne peut pas se conclure par voie électronique, soit en raison d'un impératif technique, soit en raison d'une règle inhérente à la prestation en cause[9].

7. Du point de vue historique, le commerce électronique est né il y a plusieurs décennies avec les échanges de données informatisés ("EDI")[10], utilisés entre les

---

[6] L'article 16 de la LCEN prévoit que : "*I. - L'activité définie à l'article 14 s'exerce librement sur le territoire national à l'exclusion des domaines suivants : 1° Les jeux d'argent, y compris sous forme de paris et de loteries, légalement autorisés ; 2° Les activités de représentation et d'assistance en justice ; 3° Les activités exercées par les notaires en application des dispositions de l'article 1er de l'ordonnance n° 45-2590 du 2 novembre 1945 relative au statut du notariat. II. - En outre, lorsqu'elle est exercée par des personnes établies dans un Etat membre de la Communauté européenne autre que la France, l'activité définie à l'article 14 est soumise au respect : 1° Des dispositions relatives au libre établissement et à la libre prestation des services à l'intérieur de la Communauté européenne dans le domaine de l'assurance, prévues aux articles L. 361-1 à L. 364-1 du code des assurances ; 2° Des dispositions relatives à la publicité et au démarchage des organismes de placement collectif en valeurs mobilières, prévues à l'article L. 214-12 du code monétaire et financier ; 3° Des dispositions relatives aux pratiques anticoncurrentielles et à la concentration économique, prévues aux titres II et III du livre IV du code de commerce ; 4° Des dispositions relatives à l'interdiction ou à l'autorisation de la publicité non sollicitée envoyée par courrier électronique ; 5° Des dispositions du code général des impôts ; 6° Des droits protégés par le code de la propriété intellectuelle.*"

[7] Huet (J.), *Encore une modification du Code civil pour adapter le droit des contrats à l'électronique : JCP G 2004, I, 178.*

[8] Directive Européenne 2000/31/CE du Parlement européen et du conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("directive sur le commerce électronique") ,[En ligne : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000879515&categorieLien=id].

[9] Huet (J.), "*Fasc. 2420 : Pratiques des Contrats Électroniques*", 26 Mai 2014, Date de la dernière mise à jour en 27 Juillet 2014, *JurisClasseur Contrats – Distribution, LexisNexis*, n°4 et s.

[10] V. Huet (J.), *Aspects juridiques de l'EDI, Échanges de Données Informatisées - Electronic Data Interchange : D. 1991, chron. 181 ; C. Xueref, et P. Brousse, Des « EDITERMS »* pour traiter les problèmes

entreprises ou avec les administrations, constituaient déjà du commerce électronique[11].

8. Dans les années 1970 à 1980, de grands réseaux à valeur ajoutée se sont mis en place, comme le réseau Swift qui relie les établissements de crédit du monde entier, ou le réseau SITA (Société internationale de télécommunication aéronautique) utilisé par les agences de voyages et les compagnies aériennes. Grace à ces réseaux, des millions d'informations étaient échangées chaque jour. Il s'agit là d'illustrations classiques majeures du commerce électronique[12]. En France, le commerce électronique s'est ouvert au grand public dans les années 80 avec la télématique[13].

9. Le sujet du commerce électronique dans le milieu juridique n'a pas manqué de donner lieu à des débats pour s'interroger sur la nécessité de mettre en œuvre des lois comme normes juridiques contraignantes régissant le commerce électronique; ou bien ouvrir la porte au « *soft law »* pour mettre à disposition des recommandations à la sécurité du commerce électronique.

10. - Le *Softlaw ou bien le droit-mou* - Il s'agit d'un "*vaste corpus documentaire composé d'actes d'origine diverse (publique, professionnelle, privée), qui ne sont dotés par eux-mêmes d'aucune force juridiquement obligatoire et qui, en somme, relèveraient d'une «infrajuridicité». Pour autant, ils sont pris en considération - et le plus souvent respectés - par leurs destinataires, et constituent quelquefois des éléments incontournables du régime juridique d'une matière donnée "*[14].

---

juridiques de l'EDI : propositions pour l'avenir, *Rev. dr. informatique et télécoms 1992-3, p. 7 ; E. Caprioli, JCl. Commercial, Échange de données informatisées, 1995.*

[11] Huet (J.), *Op. cit.*, n°49 et s.

[12] *V.* Huet (J.), *Aspects juridiques de l'EDI, Échanges de Données Informatisés - Electronic Data Interchange : D. 1991, chron. 181*

[13] Huet (J.), *Op. cit.*, n°4.

[14] DOUVRELEUR (O.), *Le soft law en matière financière : le point de vue de l'Autorité des marchés financiers, Revue de Droit bancaire et financier* n° 1, Janvier 2012, dossier 5, n°3.

11. L'importance de ces textes a surgi en matière financière dans les années 90 suite aux grandes crises financières, telles que les affaires *Enron* et *World Bank*[15], et l'urgence d'intervenir et traiter de la gouvernance des sociétés cotées, de la rémunération de leurs dirigeants, en s'en tenant aux seules dispositions du Code de commerce, sans évoquer les recommandations issues des acteurs eux-mêmes et de leurs organisations représentatives (Rapports Viénot, Rapport Bouton, Code Afep-Medef). Ils renvoient aussi à la notion d'autorégulation dont ils sont la manifestation et l'instrument[16].

12. Texte phare du « Softlaw » en matière du commerce électronique, la loi-modèle de la CNUDCI (Commission des Nations unies pour le droit commercial international)[17] du 1996, malgré son titre très ambitieux, concerne essentiellement les questions de preuve et de formalisme. Mais elle s'est enrichie progressivement par un curieux phénomène d'agglutination, de dispositions nouvelles concernant des questions qu'il a postérieurement été décidé de traiter : la signature électronique et services de certification.

13. Au niveau européen, les contrats électroniques sont régis par la directive sur la protection des consommateurs dans les contrats conclus à distance[18]qui prévoit le droit de rétractation de quatorze jours[19]. Il faut aussi compter avec, d'une part, une directive du 13 décembre 1999 sur les signatures électroniques pour

---

[15] V. BOURETZ (E.), « *La défaillance de la régulation financière* », *Revue de Droit bancaire et financier* n° 5, Septembre 2009, dossier 26, n°12.

[16] L'Association Française des marchés financiers (AMAFI) estime que l'autorégulation est en mesure d'apporter une réponse à l'insécurité juridique que peut faire naître l'approche « *Principle based* ». Elle permettrait ainsi « de proposer, au travers de codes professionnels notamment, des voies de déclinaison d'un principe normatif. V. Emmanuelle BOURETZ, "*La défaillance de la régulation financière* », *Revue de Droit bancaire et financier*, n° 5, Septembre 2009, dossier 26, n°10 et 11.

[17] Créée en 1966, la Commission des Nations Unies pour le droit commercial international (CNUDCI) est un organe subsidiaire de l'Assemblée générale des Nations Unies chargé d'encourager l'harmonisation et l'unification progressives du droit commercial international. Depuis sa création, elle a élaboré nombre de conventions, de lois types et d'autres instruments ayant pour objet le droit matériel applicable aux opérations commerciales ou d'autres aspects du droit des affaires qui ont une incidence sur le commerce international. Elle se réunit une fois par an, normalement l'été, en alternance à New York et à Vienne.

[18] Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil, Journal officiel de l'Union européenne, [En ligne : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32011L0083].

[19] Article 9 prévoit que « … le consommateur dispose d'un délai de quatorze jours pour se rétracter d'un contrat à distance ou d'un contrat hors établissement sans avoir à motiver sa décision...). Sur ce texte V. *A. Debet, Des nouvelles règles encadrant les contrats à distance, Comm. comm. électr. 2012, étude n° 8 et V. infra n° 65.*

assurer la libre circulation de celles-ci, par la reconnaissance mutuelle des agréments de tiers certificateurs délivrés dans les États membres, et surtout, d'autre part, une directive du 8 juin 2000, qui traite aussi bien de l'application de la loi du pays d'origine au prestataire, ou des informations devant être fournies par ce dernier lorsqu'il met en place un site internet, que du processus de conclusion des contrats électroniques[20].

14. En France, le droit positif s'est enrichi de la loi sur la confiance dans l'économie numérique *(L. n° 2004-575, 21 juin 2004[21])*, qui a introduit les articles 1108-1[22] et 1108-2[23] sur la validité des actes juridiques conclus sous forme électronique ; et les articles 1369-1 et suivants dans le Code civil pour reconnaitre l'utilisation de la voie électronique pour mettre à disposition des conditions contractuelles ou des informations sur des biens ou services (loi transposant la directive communautaire de 2000 sur le commerce électronique).

15. Ainsi l'intérêt de la présente recherche est de promouvoir d'une manière générale les communications électroniques dans le commerce international, et puis à titre particulier de présenter et étudier les nouveaux défis qui relèvent de l'utilisation des 'documents transférables électroniques', en réfléchissant sur les méthodes à adopter afin de remédier aux éventuelles déficiences technologiques, ainsi que de combler les lacunes juridiques qui ne cessent de se révéler.

16. - **Notion de 'Documents Transférables Electroniques'** - C'est un concept inventé par la CNUDCI[24]qui renvoie d'une manière générale à l'équivalent électronique d'un instrument transférable (négociable ou non négociable) ou

[20] Huet (J.), "*Fasc. 2420 : Pratiques des Contrats Électroniques*", 26 Mai 2014, Date de la dernière mise à jour en 27 Juillet 2014, *JurisClasseur Contrats – Distribution, LexisNexis*, n°5.
[21] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1), version consolidée au 15 novembre 2016, [En ligne : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164].
[22] Article 1108-1 du Code civil prévoit que : « *lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4 et, lorsqu'un acte authentique est requis, au second alinéa de l'article 1317. Lorsqu'est exigée une mention écrite de la main même de celui qui s'oblige, ce dernier peut l'apposer sous forme électronique si les conditions de cette apposition sont de nature à garantir qu'elle ne peut être effectuée que par lui-même* ».
[23] Article 1108-2 du Code civil prévoit que « *il est fait exception aux dispositions de l'article 1108-1 pour : 1° Les actes sous seing privé relatifs au droit de la famille et des successions ; 2° Les actes sous seing privé relatifs à des sûretés personnelles ou réelles, de nature civile ou commerciale, sauf s'ils sont passés par une personne pour les besoins de sa profession* ».
[24] Voir *supra* n°12.

d'un document titre. Nous sommes ici à la recherche des moyens pour pouvoir remplacer certains documents, ayant déjà une valeur juridique probante dans leur forme manuscrite, par des documents sous forme électronique qui seraient revêtus de la même protection juridique que leurs équivalents sous forme papier.

17. Nous entendons d'abord par 'instruments transférables négociables' des instruments financiers qui peuvent contenir un engagement inconditionnel de payer une somme déterminée au porteur ou ordonner à un tiers de payer le porteur. C'est le cas d'un chèque, d'une lettre de change ou d'un billet à ordre. Ces différents instruments de paiement sont des effets de commerce, revêtant des caractéristiques particulières dans leur formation et leur exécution, ainsi que dans le rapport juridique liant le titulaire du titre de l'institution financière qui lui en fournit. Pour utiliser les chèques ou les lettres de change dans un environnement informatique, nous avons besoin de dématérialiser ces titres financiers pour les rendre accessibles sur le réseau, et procéder à la transaction par voie informatique.

18. D'autre part, il y a les documents titres qui prouvent dûment que la personne en leur possession est autorisée à recevoir, à détenir et à disposer du document et des biens meubles corporels qui y sont indiqués ; tel est le cas d'un Connaissement, d'un Récépissé d'entrepôt ou encore d'un bon de livraison.

19. Exemple de Connaissement - Evoquons à titre d'exemple le connaissement dans le transport maritime. Il s'agit d'un titre qui représente les marchandises vendues, dans la mesure où celui qui détient le connaissement acquiert la propriété sur les marchandises faisant l'objet de l'opération[25]. La question essentielle concernant la possibilité d'établir avec certitude l'identité de la personne qui détient le document titre, et qui aura le droit de réclamer ses droits acquis en vertu de ce titre. Cette question met en évidence la nécessite de garantir l'unicité du document électronique représentatif de la propriété des marchandises dans l'exemple de connaissement.

[25] Stoufflet (J.), « *Fasc. 1080 : CRÉDIT DOCUMENTAIRE* », 10 Novembre 1998, Date de la dernière mise à jour : 27 Septembre 2015, *JurisClasseur Banque - Crédit – Bourse, LexisNexis,* n°40 et s.

20. Concernant le rapport 'document papier-document électronique', tout document papier dispose de caractéristiques particulières qui le distingue du 'document équivalent électronique', en lui donnant à première vue une supériorité par rapport à ce dernier. Un document papier transférable opère une réification de la valeur ou de l'obligation qu'il représente, i.e. l'obligation de payer une somme d'argent ou de livrer des marchandises est consignée dans le document écrit, et le possesseur légitime du document - le porteur - a le droit d'en assurer l'exécution et d'en tirer parti.

21. Tangibilité d'un document écrit. Une autre différence par rapport au document électronique, le document écrit lui-même est un document tangible, ce qui représente un avantage en soi. Cependant sa valeur réside non pas dans ses caractéristiques physiques mais dans les droits qui y sont consignés. Ceci nous incite à nous interroger sur le point de savoir si la possession d'un document transférable est nécessaire ou non pour l'exécution des droits.

22. Définition de l'intégrité – Les notions susmentionnées de la possession et la tangibilité d'un document sont prises en compte pour mesurer l'intégrité d'un document. Cette intégrité pour les 'documents transférables électroniques' représente l'épreuve majeure du présent travail de recherche. Ce concept d'intégrité est présent dans l'article 1316-1 du Code civil[26] sans qu'une définition soit énoncée. Si le terme d'intégrité est quelquefois employé dans les textes juridiques (V. par exemple, *Const. 4 oct. 1958, art. 16*), il n'y est pas défini à l'exception de l'arrêté du 4 janvier 2002 relatif à la déclaration d'échanges de biens (DEB) qui énonce l'intégrité comme permettant au déclarant de "*s'assurer que les données enregistrées par le centre de collecte sont identiques aux données qu'il a transmises*"[27].

23. Les normes techniques ont apporté plus des précisions, car selon la norme française d'archivage électronique '*NF Z42-013*', l'intégrité est définit comme

[26] L'article 1316-1 du Code civil prévoit que « *L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ».

[27] Arrêté du 4 janvier 2002 modifiant l'arrêté du 17 mars 1992 relatif aux conditions auxquelles doivent satisfaire les abattoirs d'animaux de boucherie pour la production et la mise sur le marché de viandes fraîches et déterminant les conditions de l'inspection sanitaire de ces établissements, *Journal Officiel* 5 Février 2002.

une "*caractéristique d'un document électronique qui n'a subi aucune destruction, altération ou modification*". C'est également la position de la norme '*ISO 15489*' sur le "record management", selon laquelle « *l'intégrité d'un document renvoie au caractère complet et non altéré de son état* ».

24. Dans ce cadre, toutes combinaisons de moyens techniques garantissant l'identification et l'intégrité sont admissibles. Les deux garanties sont le résultat à atteindre mais les moyens restent libres voire nombreux sur le marché.

25. Cycle de vie des documents électroniques. En décrivant le cycle de vie de l'acte électronique, il convient de le subdiviser en trois phases : 1) d'abord la création lorsque l'article 1316-1 du code civil[28] a employé le terme "établi" pour décrire l'écrit sous forme électronique étant admis en preuve au même titre que l'écrit sur support papier ; 2) la transmission puisque l'article 1316[29] envisage les modalités de transmission et ; 3) la conservation visée par l'article 1316-1.

26. Par la suite, toute démarche de sécurisation pendant le cycle de vie d'un acte sous forme électronique se traduit généralement par le balancement entre les deux garanties d'identification et d'intégrité :

- au moment de la création de l'écrit électronique à titre de pré-constitution de preuve, l'identification est prééminente, aussi bien que l'intégrité qui est surtout nécessitée par l'absence de support de la forme électronique ;
- pendant l'échange, l'identification ne doit pas être perdue de vue, de même que l'intégrité de l'écrit ne doit pas être remise en cause ;
- à l'étape de conservation, l'identification de l'auteur de chaque écrit doit être acquise et constante. Par contre, il faudra conserver les archives pendant un temps plus ou moins long. En cas de besoin, notamment pour l'administration de la preuve, l'archive devra être dans l'état d'origine : l'intégrité est prédominante dans cette étape, pour les besoins de la preuve en cas de survenance d'un conflit.

[28] Article 1316-1 du Code civil prévoit que "*L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité*".
[29] Article 1316 du Code civil prévoit que "*La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission*".

27. - Validation de l'écrit électronique – La validation fait suite à la formation de l'acte dématérialisé. Comme le deuxième chapitre consacré à la signature électronique et le droit de la preuve aux technologies de l'information l'envisagera en détail, il suffit ici de signaler que, comme tout document juridique porte impérativement une signature, il est devenu assez répondu aujourd'hui l'usage de la signature électronique permet de valider le document électronique.

28. - Circulation des documents transférables - Le transfert par livraison est la norme pour la circulation effective des documents transférables. Les instruments négociables, tels que les lettres de change et les billets à ordre, se négocient normalement par transfert de possession de l'instrument par une personne autre que l'émetteur à une autre qui en devient ainsi le porteur.

29. - Phase de la conservation du document électronique - Quant au dernier stade de vie d'un acte électronique ; c'est la phase de conservation. À l'issue de la conclusion du marché, tous les documents relatifs à la transaction accomplie devront être archivés. L'article 1316-1 du Code civil fait l'impasse sur cette question en soulignant l'exigence juridique de conservation qui se traduira par l'emploi de l'archivage électronique.

30. - Problématique – Les caractéristiques essentielles du document papier transférable soulèvent plusieurs questions qui représentent des obstacles à la création, à l'utilisation, au transfert et à l'exécution des 'documents transférables électroniques', et qui doivent être traitées pour permettre la création de 'documents transférables électroniques' équivalents et leur circulation avec confiance sur le marché.

31. Pour ce faire, il convient d'évaluer la faisabilité d'établir d'un cadre législatif uniforme visant à appuyer le développement des arrangements contractuels actuellement mis au point pour remplacer par des versions électroniques les documents traditionnels sur papier. Seront donc abordées les principales questions juridiques liées à la création, à l'utilisation et au transfert de 'documents électroniques'.

32. La mise en application d'un 'document transférable électronique' suscite en effet des problèmes bien distincts, comme celui de la preuve de la validité et de l'intégrité de l'écrit électronique. Afin de proposer des solutions, il convient de présenter les normes générales applicables aux documents sous forme manuscrite et les confronter aux caractéristiques spécifiques des documents électroniques. Cette méthode nous permettra de mesurer les décalages entre l'univers classique des documents papiers et celui numérique représenté par les documents électroniques.

33. Domaine de l'étude - Dans le cadre de la présente recherche, nous nous contenterons de présenter les documents transférables électroniques les plus courants et ceux qui sont considérés comme les plus utilisés dans les pays en développement. Ces derniers sont les lettres de changes, les billets à ordre et les récépissés d'entrepôt électronique.

34. Bien que le chèque électronique fasse effectivement partie de "documents transférables électroniques" il ne sera pas inclus dans la présente étude ; ceci est justifié par les raisons suivantes : nous nous somme rendu compte que l'utilisation du chèque est devenue de plus en plus restreinte, et découragée sur le marché, voire même désuète dans certaines circonstances et certains endroits ; la pratique nous montre que le marché est devenu plus méfiant que jamais à l'égard de la circulation des chèques comme instrument commercial pour régler les factures et les commandes achetées par les clients et les simples consommateurs.

35. Un document titre qui ne fera pas non plus l'objet de la présente recherche est le connaissement électronique dans le secteur du transport maritime, le connaissement et les crédits documentaires sont des sujets beaucoup trop larges pour être traités dans un cadre restreint et il convient de les mettre en évidence dans une étude séparée.

36. Plan général – Notre sujet porte sur les 'documents transférables électroniques', qui sont les effets de commerce (lettres de change/billets à ordre), warrants et récépissés d'entrepôt. Dans la première partie nous traitons de leur formation et

dans la seconde partie de l'équivalence fonctionnelle de ces documents électroniques.

37. Plan – Dans ***première partie***, dans un premier temps, nous examinerons les principes fondamentaux qui relèvent de la liberté de communication par voie électronique et de la protection de la vie privée; celles-ci constituent les piliers du commerce électronique (***Chapitre 1er***). Nous présentons, par la suite, les critères de validité des documents électroniques, et les règles de la preuve, s'y rapportant ce qui inclue la signature électronique et les procédures de certification. Ces éléments visent à garantir l'authenticité et l'unicité de l'acte électronique. Mais pour établir la confiance des usagers dans leurs transactions par voie électronique, il faut recourir à des intermédiaires de confiance, appelés "prestataires de service de confiance". (***Chapitre 2***).

38. Dans la ***deuxième partie***, nous observons qu'il y a d'autres obstacles au développement du commerce électronique et à la circulation des "documents transférables électroniques". Ceux-ci sont liés à la difficulté d'établir une équivalence fonctionnelle au document papier, pertinente à mettre en œuvre dans un environnement informatique ; ainsi nous envisageons d'une part, l'unicité technique du "document transférable électronique", comme critère fonctionnel équivalent à l'authenticité du document papier ; d'autre part, une possession technique du document électronique se construit et permet de forger le critère de contrôle, désigné comme l'équivalent fonctionnel de la possession matérielle des documents papier (***Chapitre 1er***). L'archivage électronique et la conservation des documents électronique sont les dernières phases dans le cycle de vie d'un document. Ils sont nécessaires pour des raisons de preuve suite à l'exécution du document électronique (***Chapitre 2***).

39. Les questions juridiques qui seront posées au fur à mesure de notre recherche ont été identifiées comme faisant actuellement l'objet de nombreuses études avancées: comme celles sur la validité juridique des contrats et autres documents financiers conclus par le biais des communications électroniques; l'identification, l'authentification et l'autorisation, en particulier dans le contexte de la gestion de l'identité; l'utilisation, la rétention et la confidentialité

des données; la valeur probante des documents électroniques et d'autres questions d'exécution; et les implications juridiques des différentes options architecturales techniques.

PREMIÈRE PARTIE

LA CRÉATION DU ‘DOCUMENT TRANSFÉRABLELE ÉLECTRONIQUE’

40. Problématique – Un ‘document transférable électronique’ constitué par l’utilisation des moyens de communications électroniques peut-il être jugé compatible avec les droits nationaux et les conventions internationales régissant l'écrit "traditionnel" sur support papier ?.

41. Techniquement, la réponse est positive. Mais juridiquement, les documents conclus par voie électronique sont généralement confrontés à une situation dans laquelle les règlementations dans certains pays accusent un retard par rapport aux développements informatiques et technologiques.

42. Dans le cadre de la réglementation des communications par voie électronique, les ‘documents transférables électroniques’ sont à l’origine d’un mode d’engagement entièrement dématérialisé, qui, seul, permet de générer des droits et obligations à l’égard des parties et constitue un fondement contractuel valable au moment de la survenance d’un litige devant les tribunaux.

43. Dès lors, pour s’assurer de la validité des ‘documents transférables électroniques’, les parties doivent dans le document exprimer leur consentement dans la création de l’acte sans ambiguïtés. Nous nous intéresserons plus précisément aux actes juridiques qui visent le transfert de fonds ; seuls les effets de commerce sont pris comme exemples dans la thèse.

44. Les parties contractantes doivent d’une part, respecter les conditions de la formation de l’acte qu’il soit une lettre de change, un billet à ordre, un warrant gage ou un récépissé d’entrepôt (Chapitre 1 : la formation du ‘document transférable électronique’) et d’autre part, respecter les exigences juridiques et techniques relevant de la signature et la cryptographie (Chapitre 2 : la conclusion du ‘document transférable électronique’).

CHAPITRE I

LA FORMATION DU ‘DOCUMENT TRANSFÉRABLE ÉLECTRONIQUE’

45. Le *'document transférable électronique'* présente certaines spécificités. D'une part, son support est différent du papier qui est classiquement la norme et, d'autre part, du fait de la distance des parties, divers ordres interviennent lors de la formation. Encore faut-il préciser ce que nous entendons par le terme « formation »[30]. En effet, même si nous ne prenons souvent pas soin de la définir, il existe d'abord une acceptation restrictive qui ne considère pour cette définition que les techniques indiquant quand, où et comment le document électronique se réalise. Ensuite, d'une manière plus large, le terme « formation » peut être attaché à la « forme », c'est-à-dire au support qui constitue un document juridique électronique, tant pour des considérations sécuritaires, de preuve, que pour des raisons d'expression et de communication.

46. Les parties dans une société d'information disposent d'une grande liberté d'expression et communication, leur permettant de choisir les moyens juridiques et techniques pour établir leurs engagements contractuels. Alors nous allons traiter en premier temps les piliers fondamentaux du commerce électronique (***section 1)***. Ensuite nous envisageons les conditions de validité du 'document transférable électronique' au regard des textes régissant les effets du commerce (***section 2)***.

[30] V. GAUTRAIS, *Le contrat électronique international- Encadrement juridique, Bruxelles, Bruylant, 2ème éd*., 2002, p. 81.

SECTION I

LES PILIERS FONDAMENTAUX DU COMMERCE ÉLECTRONIQUE

47. La possibilité de contribuer au contenu, de participer, réagir sur des blogs ou forum de discussion de plus en plus nombreux, fait que l'internet est devenu une partie inséparable de la vie quotidienne de l'internaute.

48. La liberté de communication par voie électronique, l'intégration de l'internet dans notre vie quotidienne et les règles législatives relatives à la liberté de communication et la liberté d'expression ont conduit au développement progressif du système juridique. Ce dernier a essayé au fil du temps de s'adapter aux nouveaux défis du commerce international et au passage à une société dite de l'information, dans laquelle les technologies de l'information jouent un rôle vital dans le commerce aussi bien au niveau interne qu'au niveau international.

49. Le principe de la protection de la vie privée, la méfiance dans l'économie numérique nous interpellent lorsque nous discutons de l'étendue de la liberté de communication et d'expression dans la société de l'information, et font ici obstacle à la liberté de communication; le respect des ces points a constamment sollicité l'intervention du législateur. (**paragraphe 1***)*

50. La présentation des effets de commerce, ainsi que les principes les régissant et les différents mouvements législatifs ayant pour objectif l'harmonisation et l'unification des règles législatives relatives aux effets de commerce, jusqu'à l'adoption des règles de la convention de la Commission des Nations Unies pour le Droit commercial international (CNUDCI) sur les lettres de change et les billets à ordre internationaux, est ainsi nécessaire avant d'aborder les moyens appropriés pour l'utilisation des effets de commerce électroniques sur le marché (**paragraphe II**).

PARAGRAPHE I LA LIBERTÉ DE COMMUNICATION PAR VOIE ÉLECTRONIQUE

I. LA LIBERTÉ SUR L'INTERNET

51. La communication par voie électronique est passée par de nombreuses phases de maturation pour atteindre sa forme actuelle de liberté. Il nous convient d'abord de présenter l'évolution de la communication des données et les moyens adoptés à chaque époque afin de parvenir à la liberté d'expression dans sa forme contemporaine issue de la société de l'information[31].

A. Présentation de l'évolution de l'internet

52. L'information est un signal porteur d'une signification : un renseignement ou élément de connaissance ne devient une information que lorsqu'il a reçu une forme qui le rend communicable. L'information est définie par l'arrêté du 22 décembre 1981 comme étant un « élément de connaissance susceptible d'être représenté à l'aide de la convention pour être conservé, traité ou communiqué[32]. »

53. De point de vue technique, l'Internet est défini comme un réseau d'interconnexion mondiale des réseaux informatiques, un réseau des réseaux[33]. Cette interconnexion généralisée des réseaux informatiques repose sur l'utilisation d'un protocole de communication commun dit TCP/IP[34]

[31] Dans ce sens, voir PERRAY (R.), *Op. cit.*, n°2.
[32] Arrêté du 22 décembre 1981 portant enrichissement du vocabulaire informatique, *JO* 10 no°1984.
[33] Internet est un système d'interconnexion de machines qui constitue un réseau informatique mondial, utilisant un ensemble standardisé de protocoles de transfert de données. C'est un réseau de réseaux, sans centre névralgique, composé de millions de réseaux aussi bien publics que privés, universitaires, commerciaux et gouvernementaux. Internet transporte un large spectre d'information et permet l'élaboration d'applications et de services variés comme le courrier électronique, la messagerie instantanée et le World Wide Web.
[34] TCP/IP est l'abréviation anglaise du terme « Transmission Control Protocol/ Internet Protocol ». Il s'agit d'un protocole de contrôle des transmissions d'informations utilisé entre machines du réseau Internet, et qui comprend une partie TCP relative à l'organisation des paquets de données et une partie IP fixant l'acheminement des données de machine à machine jusqu'à leur destination finale. In Grenité (Michel), Dictionnaire de la micro-informatique.

54. Sans entrer dans des détails techniques inutiles pour notre recherche, il s'agit tout de même d'avoir une juste compréhension de l'Internet, de son fonctionnement, des services et des informations qu'il abrite pour pleinement saisir les enjeux de sa régulation et plus spécifiquement le rôle normatif des acteurs de l'Internet.

55. Si tout le monde connait et utilise l'internet, devenu inséparable de notre quotidien, il n'est pourtant pas anodin d'en rappeler les caractéristiques. L'internet peut se présenter comme un réseau informatique mondial permettant de rendre accessible au public des services. Les services primaires qui relèvent de l'internet sont surtout le *World Wide Web (WWW)* qui correspond aux sites, et le courrier électronique (*E-mail*) qui permet d'envoyer des messages à caractère privé, comparable au courrier postal.

56. D'autres services, associés à l'internet, sont aussi très utilisés pour les échanges de fichiers. Il s'agit des systèmes de partage de fichiers poste à poste ou pair à pair ou encore *peer-to-peer*[35].

57. Techniquement, l'internet utilise le protocole de communication IP (*Internet Protocol*). Et si l'internet est en principe un réseau public, il peut permettre des correspondances privées par le service du courrier électronique, mais aussi par l'intranet qui assure un usage privatif du réseau. La confidentialité peut être assurée et doit même être respectée. Des règles spécifiques s'appliqueront alors comme le secret des correspondances, l'injure non publique, distincte de l'injure publique.

58. L'accès à l'internet est toujours assuré par un fournisseur d'accès qui propose de conclure un contrat d'accès à l'internet. Le service d'accès est assuré grâce à divers moyens de télécommunications : soit filaire (réseau téléphonique à bas

[35] Le téléchargement via des réseaux peer-to-peer (P2P ; en français, « de pair en pair » ou « égal a égal » est l'une des nouvelles problématique majeures en matière de contrefaçon sur Internet concerne; une technique de transfert illégal de fichiers informatiques d'un ordinateur à un autre, sans nécessairement passer par l'entremise d'un serveur. Elle permet à deux personnes de communiquer ensemble sur le réseau, et ainsi de faire passer de l'une à l'autre toutes sortes de fichiers numériques, comme un échange de la main à la main dans l'univers physique. Sur ce sujet, voire aussi : Vincent Fauchoux – Pierre Deprez, *Le droit de l'Internet*, *LexisNexis SA*, 2008, n°88.

débit, ADSL, ou xDSL, câble coaxial, fibre optique, courant électrique porteur CPL) soit sans fil (Wifi, Wimax, internet par satellite, 3G, 4G…).

59. Historiquement, le Web a été inventé en 1989 par Tim Berners-Lee, un ingénieur britannique travaillant au *CERN* (Centre Européen de Recherche Nucléaire). Nous citerons ici la déclaration considérée comme visionnaire de Tim Berners-Lee[36] sur son aperçu futuriste de voir l'internet :

« *J'ai fait un rêve pour le Web [dans lequel les ordinateurs] deviennent capables d'analyser toutes les données sur le Web — le contenu, liens, et les transactions entre les personnes et les ordinateurs. Un « Web Sémantique », qui devrait rendre cela possible, n'a pas encore émergé, mais quand ce sera fait, les mécanismes plan-plan d'échange, de bureaucratie et de nos vies quotidiennes seront traités par des machines dialoguant avec d'autres machines. Les « agents intelligents » qu'on nous promet depuis longtemps vont enfin se concrétiser* »

60. Cette déclaration de Tim Berners-Lee revêt un caractère aussi révolutionnaire que futuriste envers le monde de l'information, parce que les idées décrites par lui en 1989 se réalisent aujourd'hui grâce au développement spectaculaire du service Web surtout au début des années 2000 ; un développement technologique qui permet effectivement aux ordinateurs de dialoguer entre eux pour le service et le confort de l'homme.

61. A partir de l'été 1991, l'invention de l'internet a été offerte au grand public dans le monde entier sans brevet ni droit, en adéquation avec la politique générale du CERN. Au début l'utilisation le Web a été réduite à la consultation à distance de pages d'informations multimédias. Ce premier mécanisme de création de Web appelé « Web 1 » était de type systématique, et son fonctionnement était très linéaire : cela signifie que le contenu proposé par un producteur s'affiche sur un site Internet consulté par des internautes. Pourtant, c'est un web passif dans la mesure où l'internaute y consomme de l'information, comme nous pouvons le faire dans une bibliothèque par exemple, sans pouvoir pour autant participer par

[36] Tim Berners-Lee, Fischetti, Mark, *Weaving the Web, HarperSanFrancisco,* 1999 (ISBN 978-0-06-251587-2).

lui-même en ajoutant des commentaires ou modifiant le contenu sur ce qui est consulté sur le site.

62. En août 2004, l'expression *WEB 2.0* a été proposée par *Dale Dougherty* de la société *O'Reilly Media* et explicitée par *Tim O'Reilly* lors d'une conférence en 2005, pour désigner une mutation du web statique (c.à.d. Web 1 dans le cadre duquel l'internaute est un simple consommateur d'informations) vers un web participatif dans le cadre duquel l'internaute devient fournisseur d'informations.

63. Pour *Tim O'Reilly*, la clef du succès dans cette nouvelle étape de l'évolution du réseau Internet réside dans l' « intelligence collective » : « *le web 2.0 repose sur un ensemble de modèles de conception : des systèmes architecturaux plus intelligents qui permettent aux gens de les utiliser, des modèles d'affaires légers qui rendent possible la syndication et la coopération des données et des services … le web 2.0 c'est le moment ou les gens réalisent que ce n'est pas le logiciel qui fait le web mais les services !* »[37]

64. Ainsi le WEB 2.0 est considéré comme une rupture dans la manière d'appréhender la diffusion du contenu : il s'agit là de voir le réseau Internet non plus comme un média de diffusion unidirectionnel (à l'instar de la télévision ou la radio) mais comme une plateforme permettant des possibilités accrues de productions, de diffusion et de consommation de contenus par les internautes.

65. Autrement dit, à la différence du mécanisme de création systématique de WEB 1, la deuxième génération de l'internet, qui porte le nom de 'Web 2.0' ou 'Web social', bénéficie d'une amélioration des technologies de cette dernière, mais accorde aussi une place prépondérante à l' « intelligence collective », véritable clé de voute du système, de sorte qu'un site internet peut n'être constitué que par les contributions des internautes et/ou le contenu d'autres sites internet[38].

---

[37] Tim O'Reilly, *"What is web 2.0*", 30 September 2005.
[En ligne : http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html; http://www.ladocumentationfrancaise.fr/dossiers/internet-monde/web2.0.shtml].

[38] Le site 'Wikipedia' est l'exemple typique du site internet qui n'est constitué que par les contributions des internautes parce qu'il est constitué des articles à nature encyclopédique sur tous les sujets, créés et édités bénévolement par des contributeurs anonymes. Il s'agit d'un projet d'encyclopédie collective établie sur

66. Le Web 2 a eu pour effet de donner une place aux internautes eux-mêmes, en leur permettant d'interagir sur le site web. Ils peuvent exprimer leur opinion, réagir, et créer eux-mêmes de l'information, souvent personnelle, diffusée au public. De plus, cette nouvelle technologie a aussi permis aux internautes d'établir des liens entre eux et même de créer des réseaux privés leur permettre de communiquer ouvertement sur le web. (Citant à titre d'exemple les forums de discussion crées par les internautes, les services *blogs*[39] et les *hashtags*[40] sur les réseaux sociaux)

67. Le fil de l'évolution du Web ne s'arrête pas là car la bataille est rude entre les experts pour se mettre d'accord sur ce qui pourra être l'avenir du web. Nous voyons naitre un concept plus avancé qui est celui de 'Web 3'; ce web 3.0 est un concept en pleine évolution et qui a fait sa première apparition dans les années 2008.

68. 'Web 3' est plus intelligent, sémantique et technologique dans le sens où il est considéré comme « l'Internet des objets » ou « l'internet des choses ». Cela signifie que ce sont les objets au service des personnes qui communiquent avec des serveurs par l'intermédiaire de capteurs au travers de l'internet ; il y a ici une relation qui se crée entre l'univers physique et l'univers numérique ; cette relation s'explique par le fait que les machines et les individus sont de plus en plus connectés entre eux.

69. Nous illustrons cette évolution technologique par l'usage des Smartphones et les tablettes. Il existe aussi désormais la connexion à Internet de nos outils de tous les jours : Par exemple, un réfrigérateur pourrait savoir qu'il manque de certains aliments, et avec l'autorisation de son propriétaire se connecter sur un site

---

Internet, universelle, multilingue et fonctionnant sur le principe du '*wiki'*, une application web qui permet la création, la modification et l'illustration collaboratives de pages à l'intérieur d'un site web.

[39] Un *blog* est un type de site *Web* utilisé pour la publication périodique et régulière d'articles. A la manière d'un journal intime, ces articles sont typiquement datés et signés, et qui permettent aux lecteurs d'ajouter des commentaires et mettre leur avis sur le sujet abordé.

[40] Sur les réseaux sociaux, le *hashtag* sert à centraliser les messages autour d'un terme bien précis. Il sert de mot-clé pour que les utilisateurs puissent commenter ou suivre une conversation. Il est créé par l'association d'un mot-dièse « # » et d'un mot ou un groupe de mots, sans espace, par exemple : « *#Aressy ; #SocialMedia* ». Les *hahtags* peuvent être crées par n'importe quel utilisateur et permettent de mettre en relation plusieurs utilisateurs autour d'une thématique, même si ceux-ci ne se connaissent pas.

marchand, faire ses courses, commander, payer et organiser la réception des marchandises[41].

70. De tout ce qui précède, nous retenons que l'internet a connu une évolution rapide aux cours des années 90 et devenu un vrai phénomène social ; et avec l'apparition de l'achat sur internet, la numérisation des œuvres et leur diffusion sur un réseau de télécommunication mondial, sous des formes très variées (comme sites internet[42], réseaux *peer-to-peer*, les *blogs*[43] etc.), la rencontre de l'internet avec le droit devrait être au rendez vous.

B. Intervention du législateur pour l'encadrement juridique du mécanisme Web - « Droit du Web »

71. Il est indispensable d'adopter des normes juridiques et des règles de conduite pour régir et sécuriser les transactions qui s'effectuent en ligne, de même qu'il est indispensable que les auteurs et le législateur fassent preuve de créativité pour établir des règles menant à trouver des solutions pertinentes à ce phénomène de la numérisation des œuvres et l'ouverture à la société de l'information.

72. Sur le plan juridique, au milieu des années 1990, aucun texte de droit ni aucune décision de justice n'évoquaient encore l'Internet. Le réseau, à cette époque, était vu par beaucoup comme une sorte de *Far West* juridique, un secteur en friche où tout était encore possible.

---

[41] En ligne : http://www.zeblogsante.com/web-3-0-definition/.

[42] Le Site internet regroupe l'ensemble de pages Web, considérées comme une des composantes majeures d'une activité sur Internet. Ces pages web peuvent être des créations, œuvre de l'esprit, se traduisant par des aspects graphiques, textuels, voire sonores, ainsi que par des développements logiciels. Le statut de ces créations obéit aux règles du droit commun, et n'a pas manqué de donner lieu à des débats juridiques et à des décisions de justice dont l'enseignement est fort utile pour éviter des litiges lors de développement de sites.

[43] Le terme *blog* vient de contraction de l'expression web log qui signifie littéralement journal Web (c'est-à-dire journal sur Internet). A l'origine, le *blog* était une forme de site internet personnel sur lequel un internaute rédige des billets d'humeur sur des sujets aussi divers que variés et sur lesquels les lecteurs peuvent rebondir en y inscrivant leurs commentaires. D'après le Forum des droits sur l'Internet, le « blog est un site personnel qui offre à chacun la possibilité d'exprimer son point de vue personnel sur un sujet particulier et, à tous les lecteurs, de réagir à celui-ci en formulant des commentaires comme dans un forum de discussion » (*Je blogue tranquille*, dossier du Forum des droits sur l'Internet, Oct. 2005, p.3) ; voir aussi : FAUCHOUX (V.) et DEPREZ (P.), *Le droit de l'Internet*, *LexisNexis SA*, 2008, n°377 et s.

73. Au moment où le grand public commençait à croire à l'impunité dans cet espace supposé libre, les juges réfléchissaient à étendre à l'internet les règles juridiques du monde réel.

74. En 1996, le juge français se trouvait en face de nombreuses questions juridiques qu'il doit aborder pour la première fois ; c'est ainsi que le juge des référés, traditionnellement considéré comme le juge de l'urgence, a été désigné comme le seul et unique 'juge de l'Internet'[44].

75. Le TGI de Paris, le 14 août 1996[45] a procédé à la première condamnation en référé pour contrefaçon de droit d'auteur sur le web. Dans cette affaire, François-Xavier Bergot, élève de l'École Nationale Supérieure des Télécommunications (ENST) a, sans autorisation, reproduit dans ses pages Web sur le serveur étudiant de l'École et favorisé une utilisation collective d'œuvres de Michel Sardou protégées par le droit d'auteur et dont les demanderesses sont cessionnaires des droits de reproduction et de représentation.

76. Cet étudiant a de même numérisé et mis en ligne sur le réseau internet les œuvres musicales dont Jacques Brel est l'auteur de textes et souvent de la musique[46]. Ainsi le juge français a adopté une nouvelle règle de droit selon laquelle toute reproduction par numérisation d'œuvres musicales protégées par le droit d'auteur et susceptible d'être mise à la disposition de personnes connectées au réseau Internet doit être expressément autorisée par le titulaire ou le cessionnaire des droits.

77. Par jugement, les juges ont bien montré pour la première fois dans l'histoire de la jurisprudence française le vide juridique sur l'internet. Ainsi sur le fondement juridique de la violation des dispositions de la loi du 30 septembre 1986 relatives à la nécessité d'une déclaration préalable de mise à disposition de

[44] FAUCHOUX (V.) et DEPREZ (P.), *Op. cit.*, n°3.
[45] Tribunal de Grande Instance de Paris, Ordonnance de référé du 14 aout 1996, RG n° 60139/96 Société Art Music France et a. c/ ENST et a. Dalloz 2015.
[46] Il s'agit de textes de chanson de J. Brel mis en ligne sans autorisation des ayants droit. Tribunal de Grande Instance de Paris, Ordonnance de référé du 14 aout 1996, Société Editions musicales Pouchenel et a. c/ Ecole Centrale de Paris (ECP) et a. *Dalloz* 2015.

services de communication audiovisuelle que le juge a statué sur l'affaire, en condamnant la violation du droit d'auteur sur le Web.

78. En effet, toute la réglementation est susceptible de s'appliquer sur l'internet, même si des ajustements sont parfois nécessaires. Le législateur, notamment européen, a en outre voulu réguler spécifiquement l'économie numérique, en adoptant par exemple dès 1997 une directive sur la vente à distance[47], une législation sur la preuve et l'écrit électronique en 1999, suivie d'une autre directive en 2000 sur le commerce électronique.

II. LA LIBERTÉ DE COMMUNICATION À TRAVERS LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

A. La liberté de communication.

79. Lorsque nous parlons de la liberté de communication, il faut mentionner la liberté de la presse et le statut de l'audiovisuel ; puisque la liberté de la presse, est considérée comme l'une des principales libertés publiques, originairement liée à la liberté de créer un journal, de publier ses opinions dans un journal ou dans un livre, elle est la caractéristique de la liberté d'expression. Ce qui fait de la liberté de la presse une notion générique essentielle d'où résulte la liberté de la communication.

80. Étant une condition nécessaire à l'exercice de la démocratie, la liberté de la communication a débuté par celle de la presse. Elle participe du droit d'expression et de critique dont disposent tous les citoyens vivant dans un pays démocratique. Il est ainsi utile de présenter l'évolution historique de la liberté en

[47] Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance. [En ligne http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:31997L0007]. La directive de 1997 a été abrogée par la Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs. [En ligne : http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32011L0083].

suivant son évolution depuis l'époque où la liberté de la presse et de l'audiovisuel firent apparition pour la première fois sur le plan juridique.

81. Pendant des siècles, l'histoire du droit de la communication concerne avant tout l'écrit –la presse et les ouvrages – et la conquête à la liberté d'expression a trouvé une évolution progressive dans le temps. Le 29 Juillet 1881 représente une date significative dans l'histoire de la liberté d'expression, puisqu'il s'agit de la date de l'entrée en vigueur de la Loi du 29 Juillet 1881 sur la Liberté de la presse[48].

82. Cette loi de 1881 est considérée comme le socle juridique fondateur de la liberté de la presse et la liberté d'expression en France, inspiré par l'article 11 de la déclaration des droits de l'homme et du citoyen du 26 Aout 1789[49]. Elle est d'ailleurs un texte qui en limite l'exercice et incrimine certains comportements spécifiques à la presse (« les délits de presse ») pour garantir sa liberté.

83. La loi du 29 juillet 1881 sur la liberté de la presse est emblématique. C'est qu'elle représente l'approche d'un compromis optimal entre l'exercice de la liberté fondamentale de l'information et la protection des droits des personnes. Le principe de liberté qu'elle édicte, encadré d'incriminations précises (i.e. la diffamation, l'injure, l'offense, la publication de fausses nouvelles, les interdictions d'informer.etc.) ainsi que les mécanismes de régulation de l'information comme l'exercice des droits de réponse et de rectification qu'elle contient[50].

84. De plus, ce qui est remarquable dans le texte de la loi de 1881 c'est qu'il est toujours applicable ; évidemment il a fait l'objet de nombreuses reformes législatives pour le moderniser et rendre le texte plus adapté à l'évolution du monde actuel. Il ne s'agit donc plus aujourd'hui d'une loi sur la liberté de la

[48] Loi du 29 juillet 1881 sur la liberté de la presse, version consolidée au 29 janvier 2014. [En ligne : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722].
[49] Article 11 de la déclaration des droits de l'homme et du citoyen du 26 Aout 1789 prévoit que « La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté, dans les cas déterminés par la Loi ».
[50] *Ibid.*

presse, mais d'une grande loi sur la liberté d'expression "publique" qui s'applique aussi bien à l'écrit, à l'audiovisuel, qu'au réseau Internet.

85. Pourtant, il convient de rappeler quel progrès fut la loi puisque jusqu'au XIIIe siècle, le droit de la presse et la liberté d'expression étaient étroitement surveillés par un système politique qui limitait rigoureusement la liberté d'expression pour entraver toute opposition éventuelle au pouvoir.

86. Pendant toute la période de l'Ancien Régime, la presse était opprimée et vivait sous la dépendance du pouvoir politique, soumise à l'arbitraire et aux « privilèges » ; une situation décrite par la célèbre *boutade de Beaumarchais* : *« Pourvu que je ne parle dans mes écrits ni de l'autorité, ni du culte, ni de la politique, ni des gens en place, ni des corps en crédit, ni de l'Opéra, ni des autres spectacles ni de personne qui tienne à quelque chose, je puis tout imprimer librement sous l'inspection de deux ou trois censeurs »* (Le Barbier de Séville, acte V, scène 3).

87. Comme il l'a bien illustré M. le Professeur **Yves BISMUTH,** dans son ouvrage '*Droit de l'Informatique – Eléments de Droit à L'usage des Informaticiens'* en décrivant cette période qui précède la révolution jusqu'à la promulgation de la loi de 1881 comme '***de la liberté proclamée à la liberté bafouée***'[51].

88. La radio fera ensuite, l'objet d'un embryon de législation, puis entre deux guerres et la libération la V^{e} République verra éclore un premier texte sur la liberté d'expression dans le cadre audiovisuel. Mais la liberté d'expression est toujours contingente des moyens techniques mis en œuvre et des pouvoirs en place qui acceptent ou pas cette expression.

[51] BISMUTH (Y.), *Droit de l'Informatique – Eléments de Droit A L'Usage des Informaticiens*, éd. *L'Harmattan*, 2011.

B. Sources de la liberté de communication

a) Sources nationales de la liberté de communication :

1) Les textes de valeur constitutionnelle

i. La Déclaration des Droits de l'Homme et du Citoyen du 26 août 1789 (DDHC)

89. la DDHC a consacré le principe de liberté de la presse dans son article 11 : « *La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme ; tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi* ».

90. Pourtant, la liberté de la presse n'est pas absolue ; le texte de la DDHC lui fait connaitre des limites, en prévoyant que : « *la liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées par la loi* [52]» (art. 4 DDHC).

91. D'autre part, la consécration des règles issues de la Déclaration des droits de 1789 a été implicitement approuvée en faisant référence à la déclaration des droits de l'homme dans les préambules de 1946 et 1958 :

ii. Préambule de la constitution du 27 octobre 1946

92. Le texte du Préambule de la constitution du 27 octobre 1946[53] il est prévu une « *réaffirmation solennelle des droits et libertés de l'homme et du citoyen consacrés par la Déclaration des droits de 1789 et les principes fondamentaux reconnus par les lois de la République* ». Ainsi en le mentionnant dans son

[52] Déclaration universelle des droits de l'homme (1948-1998). [En ligne : http://www.assemblee-nationale.fr/histoire/dudh/1789.asp].
[53] Constitution de 1946, IVe République. [En ligne : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/la-constitution/les-constitutions-de-la-france/constitution-de-1946-ive-republique.5109.html].

préambule, la constitution française de 1946 a effectivement conféré une valeur constitutionnelle à la DDHC de 1789, et par conséquent, aux principes de la liberté d'expression et de la presse.

iii. Préambule de la Constitution du 4 octobre 1958[54]

93. Le Préambule de la Constitution du 4 octobre 1958 dispose que : « *le peuple français proclame solennellement son attachement aux droits de l'homme et aux principes de la souveraineté nationale tels qu'ils ont été définis par la Déclaration de 1789 et complétés par le préambule de la Constitution de 1946* ». Or, dans le sens de cet article, nous apercevons clairement une autre confirmation de la reconnaissance et l'attachement aux principes de la liberté qui découlent de la DDHC de 1789.

2) Sources jurisprudentielles.

94. Concernant la jurisprudence constitutionnelle française, le Conseil constitutionnel, ayant pour objectif principal la vérification de la conformité de la loi à la Constitution, affirme que le texte de la loi est en mesure de respecter d'autres textes et principes qui portent la même valeur constitutionnelle ; l'ensemble constituant le « bloc de constitutionnalité » que les lois devraient toujours garder respect.

95. Dans une décision du 16 juillet où une loi déférée à l'examen du Conseil constitutionnel par Alain Poher, le président du Senat, a été soumise au vote des deux assemblées, dans le respect d'une des procédures prévues par la Constitution, au cours de la session du Parlement ouverte le 2 avril 1971. Il demandait au Conseil constitutionnel de se prononcer sur la conformité de ce texte à la Constitution.

96. En fait, les associations en France étaient placées sous le régime de la loi de 1901. Les associations peuvent se former librement, sans contrôle de

[54] Constitution du 4 octobre 1958. [En ligne : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/la-constitution/la-constitution-du-4-octobre-1958/texte-integral-de-la-constitution-du-4-octobre-1958-en-vigueur.5074.html].

l'Administration, mais peuvent être reconnues par l'État avec une simple déclaration en préfecture, en vertu du principe de la liberté d'association.

97. En 1971, certains artistes décident de créer des associations inspirées par l'idéologie communiste. L'administration s'oppose ainsi à la déclaration de l'association Les "Amis de La Cause du peuple", en refusant de délivrer le récépissé de déclaration sans aucune base légale. Le ministre de l'Intérieur Raymond Marcellin soupçonnait l'association d'être une organisation gauchiste se proposant de reconstituer une association dissoute qui s'appelait "La Cause du peuple". Le Gouvernement décide alors de faire voter une loi pour instituer un contrôle administratif de la déclaration des associations. Cette loi tendant à compléter les dispositions des articles 5 et 7 de la loi du 1er juillet 1901 relative au contrat d'association.

98. Dans sa décision fondatrice du 16 juillet 1971[55] le Conseil constitutionnel a réagi comme protecteur des droits et libertés des citoyens, puisqu'il a reconnu la valeur constitutionnelle du préambule de la Constitution de 1958, lequel renvoie à la DDHC de 1789 et au Préambule de la Constitution de 1946, c'est-à-dire à la plupart des textes et principes relatifs à la protection des libertés publiques.

99. Dans cette même décision, le conseil constitutionnel a fait référence aux « principes fondamentaux reconnus par les lois de la République » ; une référence considérée floue et imprécise par sa généralité, et qui englobe les grandes lois de la III^{e} République, dont la loi du 29 juillet 1881 faisait partie.

100. Se référant aussi à l'article 11 de la Déclaration des droits de l'homme de 1789, le juge constitutionnel estime « *qu'il appartient au législateur de concilier en l'état actuel des techniques et de leur maitrise, l'exercice de la liberté de communication avec, d'une part, les contraintes techniques inhérentes aux moyens de communication audiovisuelle et, d'autre part, les objectifs de valeur constitutionnelle que sont la sauvegarde de l'ordre public, le respect de la*

[55] Décision n° 71-44 DC du 16 juillet 1971. [En ligne : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1971/71-44-dc/decision-n-71-44-dc-du-16-juillet-1971.7217.html].

liberté d'autrui et la préservation du caractère pluraliste des courants d'expression socioculturels auxquels ces modes de communication, par leur influence considérable, sont susceptibles de porter atteinte » (Considérant 5 de la décision du 16 juillet 1971).

101. Cette déclaration précieuse du juge constitutionnel a été reprise ultérieurement par une autre décision du conseil constitutionnel rendue le 27 juillet 2000[56] en accordant au législateur le soin de « *concilier la liberté de communication avec la protection de la liberté d'autrui et la sauvegarde de l'ordre public* ».

102. Dans cette affaire, plus de soixante députés à l'assemblé déféraient au Conseil constitutionnel la loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication et mettant en cause plusieurs dispositions préexistantes. Cette dernière décision réaffirme dans les mêmes termes l'ensemble des principes relatifs à la protection des libertés publiques ; de même que la décision faisant suite à une question prioritaire de constitutionnalité (QPC).

103. Le Conseil constitutionnel a réaffirmé que « *les atteintes portées à l'exercice de la liberté de communication doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi* ». Nous saisissons par là l'affirmation de la valeur essentielle de la liberté de communication s'accompagne souvent de la référence à la nécessaire conciliation de cette liberté avec celle des autres ; que toutes dérogations, voire des restrictions à la liberté de communication et d'expression doivent être nécessaires, justifiées par un objectif valable, appropriées et proportionnées.

[56] Décision du Conseil constitutionnel n° 2000-433 DC du 27 juillet 2000 modifiant la Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication. [En ligne : http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=8451AEF6764B35C1295707CA9DDDA8CA.tpdjo08v_2&dateTexte=?cidTexte=JORFTEXT000000583643&categorieLien=cid].

b) Les sources européennes et internationales

104. En droit international, les législations relatives à la liberté d'expression et la protection des personnes à l'égard du traitement des données à caractère personnel sont nombreuses. Nous réduisons notre présentation aux seules sources principales de la liberté d'expression au niveau international.

105. Certains textes sont considérés comme les piliers fondamentaux de la liberté de communication et d'expression au niveau international (1) D'autres plus spécifiques portent sur la protection des données à caractère personnel (2).

1) Textes fondamentaux portant sur les droits de l'homme et la liberté d'expression

106. Deux sources majeures ont marqué l'histoire de la liberté d'expression au niveau international. Bien qu'elles aient une nature juridique différente, il s'agit d'abord de la Déclaration universelle des droits de l'homme de 1948[57] ; puis du Pacte international relatif aux droits civils et politiques de 1966[58].

i. La Déclaration universelle des droits de l'homme du 10 décembre 1948

107. L'idée d'une Déclaration universelle des droits de l'Homme fut acceptée dès la fin de la Conférence de San Francisco en date du 26 juin 1945. Cette généreuse proposition doit son succès à deux personnes qui ont joué un rôle majeur dans son aboutissement: il y a d'abord Anna Eleanor Roosevelt, une femme politique américaine, l'épouse du président américain Franklin Roosevelt et la première dame des Etats Unis du 4 mars 1933 au 12 avril 1945. Elle était très connue à l'époque en tant que 1re présidente de la Commission présidentielle américaine sur le statut de la femme et elle a présidé la

[57] Déclaration universelle des droits de l'homme de 1948. [En ligne : http://www.textes.justice.gouv.fr/textes-fondamentaux-10086/droits-de-lhomme-et-libertes-fondamentales-10087/declaration-universelle-des-droits-de-lhomme-de-1948-11038.html].

[58] Pacte international relatif aux droits civils et politiques de 1966. [En ligne : http://www.assemblee-nationale.fr/histoire/peinedemort/pacte-international-droits-civils-et-politiques.asp].

commission chargée de rédiger la Déclaration universelle des droits de l'homme[59]. L'autre personne qui a contribué au succès de la déclaration est le juriste français René Cassin qui était à l'époque le vice-président du Conseil d'Etat, et il est considéré comme l'artisan majeur de la Déclaration[60].

108. Ainsi après de longs travaux préliminaires, l'Assemblée Générale des Nations Unies se réunit solennellement à Paris au Palais de Chaillot en présence du président de la République française Vincent Auriol et adopte le texte de la Déclaration universelle des droits de l'Homme en 10 décembre 1948.

109. La déclaration fait expressément référence à la liberté d'opinion et d'expression dans l'article 19 [61]: « *Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit.* ».

110. Nous retenons ici que cette définition a un champ d'application très large en adoptant une notion vaste de la liberté de communication et d'expression, pour pouvoir y inclure non seulement la liberté d'expression, mais également celle de recevoir et de rechercher des informations sans considération de frontières ; ce qui est d'ailleurs intéressant puisque l'accès à Internet est considéré comme un droit de l'homme, une règle de droit initiée par la Directive du parlement européen, et ainsi reconnaitre la liberté de communication par voie électronique.

111. Cette Déclaration de 1948 vise à assurer « *le respect universel et effectif des droits de l'homme et des libertés fondamentales* », en marquant ainsi la reconnaissance de droits économiques et sociaux. Ce qui est pourtant regrettable c'est que ce texte n'a qu'une valeur morale et symbolique, puisqu'elle n'a pas

[59] Histoire de Anna Eleanor Roosvelt. [En ligne : https://www.whitehouse.gov/1600/first-ladies/eleanorroosevelt].
[60] Histoire de la rédaction de la DUDH. [En ligne : http://www.un.org/fr/sections/universal-declaration/history-document/index.html].
[61] La Déclaration universelle des droits de l'homme de 1948, site officiel des *Nations Unies*. [En ligne : https://www.un.org/fr/documents/udhr/index.shtml].

de valeur juridique contraignante comme son équivalent en France (la Déclaration de Droits de l'Homme et du Citoyen « DDHC ») de 1789 et ne prévoit ainsi aucune sanction.

112. Cependant ce texte instaure une exigence morale ainsi que le principe de l'universalité des droits de l'homme, ce qui signifie que les valeurs inscrites dans la Déclaration universelle doivent être respectées quels que soient le lieu, le régime politique, la religion, etc.

113. Nous concluons que cette déclaration est une preuve de reconnaissance de la dignité et de la liberté de l'être humain et apparaît comme une réponse aux vœux de René Cassin qui écrivait : « *Ainsi c'est l'homme tout entier dont les facultés et les prérogatives indispensables au développement de sa personnalité physique, intellectuelle et morale, doivent être reconnues et protégées* [62]»

ii. Le Pacte international relatif aux droits civils et politiques du 16 décembre 1966[63]

114. Il s'agit d'une convention internationale, adoptée sous forme de traité par l'Assemblée générale des Nations Unies le 16 décembre 1966, pour donner force juridique aux principes de la Déclaration universelle des droits de l'homme de 1948.

115. Le Pacte de 1966 comprend les droits et libertés classiques qui protègent les particuliers contre les ingérences de l'État, comme le droit à la vie, l'interdiction de la torture, de l'esclavage et du travail forcé et le droit à la liberté et la liberté d'expression et de communication.

116. Ce texte est entré en vigueur le 23 mars 1976, et ratifiée par 167 Etats, dont la France par la loi du 25 juin 1980[64]. C'est ainsi qu'à la différence de la

[62] Qu'est-ce-que la déclaration universelle des droits de l'Homme de 1948. [En ligne : http://www.crdp-montpellier.fr/ressources/99/99dh0103.html].
[63] Pacte international relatif aux droits civils et politiques du 16 décembre 1966, entrée en vigueur: le 23 mars 1976 ; Haut-commissariat aux droits de l'homme, *Nations Unies Droits de l'homme.* [En ligne : http://www.ohchr.org/FR/ProfessionalInterest/Pages/CCPR.aspx].
[64] Plateforme d'information human rigts.ch. [En ligne : http://www.humanrights.ch/fr/Instruments/ONU-Traites/Pacte-II/index.html].

Déclaration universelle des droits de l'homme de 1948, le Pacte a une force contraignante et ses dispositions doivent être respectées par les Etats membres sous peine de sanctions.

2) Textes spécifiques portant sur la protection des données à caractère personnel

117. La compréhension des principes de la réglementation relative à la protection des données à caractère personnel part d'un constat : celui de la généralisation de l'outil informatique dans le quotidien.

118. Ces données personnelles se circulent à travers des systèmes informatisés permettant à leurs utilisateurs de ressembler et accumuler en un espace restreint un nombre considérable d'informations, afin soit de les réutiliser en un temps très court ou de les conserver sur une longue durée.

119. Ce qui est encore plus rentable et bénéfique pour les utilisateurs d'utiliser les outils informatiques la possibilité de mettre en relation toutes leurs données centralisées dans un système. Ces systèmes informatisés deviennent ainsi une source riche d'informations, y compris pour soi-même avec le développement des objets connectés[65].

120. Lorsque ces données personnelles appartenant aux clients font de manière quotidienne l'objet de multiples opérations de collecte, de transfert et, plus généralement de traitement sur Internet, il va falloir élaborer des règles pour régir l'utilisation de ces données personnelles qui appartiennent à des personnes privées, ainsi que de garantir la protection de leur données sur le réseau.

[65] *CNIL, Quantified self, m-santé : le corps est-il un nouvel objet connecté ? 28 mai 2014 : www.cnil.fr ; Comm. com. électr. 2014, alerte 49, note F. Meuris*. - V. pour plus de détails, *N. Weinbaum, Les données personnelles confrontées aux objets connectés : Comm. com. électr. 2014, étude 22. - Groupe de l'article 29, avis n° 8/2014, 16 sept. 2014, WP 223.* - V. d'une manière plus générale, *M. Touchard, Nous aurons à l'aube de 2020 près de 50 milliards d'objets connectés, une tendance à ne pas ignorer - 3 Questions à Me Thierry Piette-Coudol : JCP G 2015, 461*. - V. sur les précautions à suivre en termes de protection, *F. Eon, Objets connectés : comment protéger les données de santé ? Comment concilier amélioration de la santé publique et le respect de la vie privée : RLDI avr. 2016, n° 125, p. 49*.

Les deux textes communautaires suivants ont largement contribué à la réglementation des données personnelles dans le cadre de l'Union européenne.

i. La Directive 95/46/CE sur la protection des données personnelles[66]

121. Considéré comme un texte de référence, au niveau européen, en matière de protection des données à caractère personnel, la Directive du parlement européen et du conseil a été publiée au Journal officiel de l'Union européenne du 23 novembre 1995.

122. La Directive 95/46/CE du 24 octobre 1995 est le premier texte communautaire qui est adopté afin d'harmoniser, dans l'ensemble des pays membres, les législations applicables à la protection des données à caractère personnel. Le texte de la Directive de 1995 est inspiré principalement des réglementations nationales déjà existantes, en apportant quelques modifications à certaines de leurs dispositions.

123. D'une part, la réforme de 1995 a instauré le principe d'égalité en matière d'obligations et de formalités s'imposant dans un pied d'égalité aux organismes du secteur public comme du secteur privé. Elle a également mis fin à la distinction entre traitements manuels et automatisés ; chacun étant désormais soumis pour l'essentiel aux mêmes principes.

124. D'autre part, la Directive de 1995 a joué un rôle indéniable pour la création du droit de l'Internet, surtout grâce au travail d'adaptation de la Commission nationale de l'informatique et des libertés (CNIL) [67], notion introduite par la loi

[66] Directive du 24 octobre 1995/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Legifrance.*
[En ligne: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000697074].

[67] La Commission nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle exerce ses missions conformément à la loi no 78-17 du 6 janvier 1978 modifiée le 6 août 2004, [En ligne : https://www.cnil.fr/en/home].

du 6 août 2004, pour instituer la CNIL qualifiée d' « autorité administrative indépendante » (AAI[68]) ;

125. C'est dans un souci de fournir une protection plus efficaces aux données personnelles au niveau européen que la Directive a ouvert la porte aux autorités nationales en charge de la protection des données personnelles, telle que la CNIL en France, en renforçant leur rôle, et leur accorder plus de pouvoirs de contrôle, qui s'exercent désormais *a posteriori* et plus seulement *a priori*, et de pouvoirs de sanction[69].

126. Grâce à la directive de 1995 la CNIL est portée compétente en la matière et peut avertir, mettre en demeure ou bien encore sanctionner le responsable du traitement qui ne respecterait pas les dispositions prévues dans la loi.

127. Afin de garantir l'autonomie de la CNIL dans l'exercice de ses fonctions, l'article 22 de la loi « informatique et Libertés » prévoit que « *dans l'exercice de leurs attributions, les membres de la commission ne reçoivent d'instructions publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent s'opposer à l'action de la commission ou de ses membres et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche* ».

128. Dans le cadre de sa mission que lui a été attribuée par la loi, la CNIL, en tant que AAI, doit remplir les fonctions suivantes :

- Le contrôle de la conformité à la Loi des projets de fichiers et traitements ;
- Le rôle de conseil et d'information ;
- L'instruction des plaintes ;

[68] Les Autorités Administrative Indépendante (AAI) constituent une catégorie juridique particulière qui ne dispose d'aucune définition légale. Il existe à ce jour plus de quarante AAI disposant d'un régime juridique hétérogène. Ces AAI sont régies par les différents textes qui les ont institués.

[69] V. notamment pour plus de précisions, D. Martin, *La directive 95/46 transposition en droit français : Gaz. Pal. 1998, 1, doctr. p. 601.* - Y. Poullet, *De quelques questions relatives à l'application de la directive données personnelles n° 95/46 du 24 octobre 1995 au contexte de l'Internet : Lamy droit de l'informatique, suppl., n° 96, oct. 1997, p. 11.* - M.-C. Ponthoreau, *La directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données : RFDA 1997, p. 125.* - J. Frayssinet, *La directive du 24 octobre 1995 : Cah. Lamy mars 1996 (K), p. 1.*

- Le pouvoir de vérification sur place ;
- Le pouvoir de sanction.

129. Ainsi, la CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

130. Citant un exemple de sujets dont la CNIL peut se saisir. S'agissant par exemple d'un centre d'appel qui exploite des données à caractère personnel dans le cadre de son activité. Dans cette hypothèse, l'archivage de ces données peut poser de multiples problématiques aussi bien au niveau juridique que technique. De plus, la protection des données dans une telle entreprise nécessite un niveau élevé de protection contre le piratage afin de sécuriser le système informatique qui utilise les données des clients. C'est la raison pour laquelle à chaque étape de traitement de données des procédures particulièrement techniques soient mises en œuvre pour protéger ces données, sources de bénéfices pour les entreprises qui les exploitent.

131. D'ailleurs, le traitement des données fait l'objet d'une déclaration qui exige une autorisation préalable ; le législateur français vise ici les fichiers dits d'exclusion ou « listes noires » qui répertorient tant des informations relatives aux incidents de paiement que des comportements pénalement répréhensibles ou encore des «anomalies» ou «incohérences»[70].

132. Ainsi la CNIL, en tant qu'autorité nationale en charge de la protection des données personnelles, contribue directement à la prospection directe en ligne, à l'élaboration de divers fichiers commerciaux et des listes noires relatives aux incidents de paiement et autres comportements répréhensibles ainsi qu'à l'activité de certains prestataires de services de confiance comme les prestataires de services de certification électronique.

[70] *Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Journal Officiel* du 7 Aout 2004, [En ligne : www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676; http://www.caprioli-avocats.com/publications/44-donnees-perso/89-loi-6-aout].

133. Il est bien de noter que le principe de la liberté de communication par voie électronique ne contredit pas le besoin de l'utilisation des données personnelles dans certaines activités ; c'est que l'enregistrement et l'utilisation des données personnelles sont au cœur même de différentes activités.

134. En France, la transposition de la directive du 24 octobre 1995 par la loi du 6 août 2004 a eu lieu près de dix après, en modifiant celle du 6 janvier 1978. Cela n'a pourtant pas empêché le Conseil d'État de se référer à la directive 95/46/CE durant cette période[71].

135. Le retard de la transposition des dispositions de la directive de 1995 en France est dû à l'intention du législateur français de maintenir un niveau élevé de protection, sans pour autant bouleverser la réglementation déjà existante[72].

136. En droit interne, le législateur français avait adopté la *loi Informatique et Libertés du 6 janvier 1978* relative à l'informatique, aux fichiers et aux libertés[73]. Un texte promulgué à la suite de l'affaire Safari[74], et qui réglemente notamment aujourd'hui la pratique du fichage, manuel ou informatique. Ce texte a été adopté et modifié dans le but de protéger les données à caractère personnel qu'une personne, physique ou morale, pourrait utiliser dans le cadre d'un traitement automatisé, ou non.

137. La loi de 1978 a donc été modifiée par la loi du 6 août 2004[75] afin d'instaurer un régime unifié de déclaration des traitements de données pour le secteur privé (entreprises et professionnels) et le secteur public, et ainsi de

---

[71] CE, ass., 30 juin 2000, n° 210412, *Ligue des droits de l'homme et du citoyen : JurisData n° 2000-060767 ; AJDA 2000, n° 10, concl. P. Fombeur ; JCP G 2000, IV, 2742 ; LPA 13 févr. 2001, n° 31, p. 10, note R. Diane ; Gaz. Pal. 10 mars 2001, n° 69, p. 21,* obs. P. Graveleau *; Gaz. Pal. 17 juill. 2001, n° 198, p. 42,* note A.-F. Godet.

[72] V. notamment pour un rappel historique détaillé, VIVANT (M.), C. Le STANC, *L. Rapp et M. Guibal, Droit du numérique : Lamy, 2014, n° 544 s.*

[73] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *Legifrance* [En ligne : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460].

[74] Le Système automatisé pour les fichiers administratifs et le répertoire des individus (dont l'acronyme est SAFARI) désignait un projet d'interconnexion des fichiers nominatifs de l'administration française, notamment par le biais du numéro INSEE, [En ligne : http://www.cnil.fr/vos-droits/histoire/].

[75] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1), [En ligne : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676].

transposer en droit français les dispositions de la Directive 95/46/CE sur la protection des données personnelles.

138. La loi modifiée de 1978 (suite à la Directive 95/46/CE et la transposition de ses règles en droit français par le biais de la Loi du 6 Août 2004) est complétée par son décret d'application n°2005-1309 en date du 20 octobre 2005[76]. Cette transposition a modifié de manière substantielle le texte de 1978, en élargissant le domaine des données qualifiées de personnelle (*article 2*), simplifie leurs régimes juridiques et alourdie les sanctions aux articles *226-16* à *226-24* du Code pénal. De plus, les pouvoirs d'enquête, d'investigation et de sanctions de la CNIL (Commission nationale de l'informatique et des libertés) sont renforcés.

ii. Le nouveau règlement européen sur la protection des données personnelles du 27 avril 2016[77]

a) Contexte et objectifs du règlement du 27 avril 2016

139. L'adoption du règlement du 27 avril 2016 représente un grand pas vers l'évolution de la liberté d'expression et pour la protection des données personnelles. Pourtant il faut attendre encore jusqu'à 2018 pour qu'il soit applicable dans tous les Etats membres de l'Union européenne.

140. Le règlement de 2016 remplacera la directive actuelle sur la protection des données de 1995 par un texte général créant un niveau élevé, renforcé et uniforme de protection des données à travers l'UE plus adapté à l'ère numérique, et d'accordera aux citoyens européens plus de contrôle sur leurs propres informations privées dans un monde numérique de téléphones intelligents

[76] Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *Legifrance*, [En ligne : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000241445].

[77] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), [En ligne : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679].

(‘*smart phones*’), de médias sociaux, de services bancaires sur Internet et de transferts mondiaux[78].

141. Dans ce contexte, le règlement propose un cadre simplifié pour les entreprises afin de procéder aux formalités administratives, ainsi que de leur offrir un cadre juridique unifié. Il est prévu à l’article 1er – alinéa 1 du règlement que son objet est d’établir des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données.

142. Alors le règlement vise à promouvoir la libre circulation des données à caractère personnel au sein de l'Union dans la mesure où la circulation des données personnelles ne pourrait plus être limitée ou interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. (article 1er – alinéa 3 du règlement).

143. Ce règlement est le résultat d’un travail ardu au sein du parlement européen et pour des quatre longues années de négociations intensives pour pouvoir aboutir à ce texte de droit. "*Grâce à ce règlement général, avoir un niveau élevé et uniforme de protection des données à travers l'UE deviendra une réalité. Il s'agit d'une victoire pour le Parlement et d'un 'oui' européen fier aux droits très forts des consommateurs et à la concurrence à l'ère numérique. Les citoyens pourront décider eux-mêmes des informations personnelles qu'ils souhaitent partager*" a déclaré Jan Philipp Albrecht, un député au parlement européen et en charge de la législation au parlement[79]. Il a aussi ajouté que "*le règlement apportera de la certitude aux entreprises grâce à une législation unique dans l'UE. La nouvelle loi 2016 renforcera la confiance et la clarté juridique et garantira une concurrence plus loyale*".

[78] Dans ce sens, l’alinéa 2 de l’article 1er du règlement prévoit que «*le règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel ».*

[79] ULDALL (R.) et de MONTIS (W.), *Réforme sur la protection des données: le Parlement approuve de nouvelles règles adaptées à l'ère numérique*, 14 Avril 2016, [En ligne : http://www.europarl.europa.eu/news/fr/news-room/20160407IPR21776/r%C3%A9forme-sur-la-protection-des-donn%C3%A9es-des-r%C3%A8gles-adapt%C3%A9es-%C3%A0-l'%C3%A8re-num%C3%A9rique].

b) Les nouveautés apportées par le règlement du 27 avril 2016

Le règlement du 27 avril 2016 a adopté des nouvelles règles que nous allons présenter dans l'ordre suivant :

1) Exigence d'un consentement clair et explicite de la personne concernée quant à l'utilisation de ses données personnelles

144. *Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale* (Considérant 32 du règlement).

145. Dans le domaine numérique il est donc nécessaire d'opter pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel.

146. De la même façon, lorsque le consentement de la personne concernée se trouve accorder à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé[80].

147. Dans la logique juridique du règlement, le silence ne vaut pas consentement, puisqu'il s'agit d'une condition de validité. Pour que le traitement de données à caractère personnel soit licite, il doit être fondé sur le consentement de la personne concernée ou reposer sur tout autre fondement légitime prévu par la loi, soit dans le présent règlement soit dans une autre disposition du droit national ou du droit de l'Union (Considérant 40 du règlement).

[80] Dans ce sens, l'article 7 alinéa 2 du règlement prévoit que *« Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante ».*

148. En cas de litige en justice mettant en question le consentement de la personne concernée, le responsable du traitement doit être en mesure de prouver que ladite personne a donné son consentement au traitement de données à caractère personnel la concernant[81] (article 7 alinéa 1er du règlement).

149. Evoquons un exemple d'un document électronique qui a subi une publication illicite de la part d'un prestataire de services de confiance, la personne titulaire du document a le droit de le poursuivre en justice du fait qu'il a publié un document à caractère personnel et qu'il a manqué à son devoir de protéger les données à caractère personnel la concernant.

150. Concernant le pouvoir discrétionnaire de retrait du consentement, la personne concernée a le droit de retirer son consentement à sa discrétion et à tout moment. Le retrait du consentement fait l'objet de l'article 7, dans son alinéa 3 le texte prévoit que *le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.* D'après ce texte, la personne n'a que simplement signaler au responsable du traitement sa volonté de retirer le consentement pour l'accorder à un autre fournisseur.

151. Il est aussi important de savoir que le règlement 2016 fixe des normes minimales sur l'utilisation des données à des fins policières et judiciaires. Ceci est évoquée dans le texte du règlement dans le Considérant 54 qui prévoit que : « *Le traitement des catégories particulières de données à caractère personnel peut être nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique, sans le consentement de la personne concernée. Un tel traitement devrait faire l'objet de mesures appropriées et spécifiques de façon à protéger les droits et libertés des personnes physiques. Dans ce contexte, la notion de «santé publique» devrait s'interpréter selon la définition contenue dans le règlement (CE) no 1338/2008 du Parlement européen et du Conseil* »

[81] Dans ce sens, le Considérant 42 du règlement prévoit que « *Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement devrait être en mesure de prouver que ladite personne a consenti à l'opération de traitement…etc.*).

2) le droit à l'oubli (droit à l'effacement)

152. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais (article 17 du règlement).

153. Lorsqu'on est dans l'hypothèse évoquée dessus sur le retrait du consentement, la personne concernée pourra demander au responsable du traitement l'effacement des données personnelles la concernant après leur transfert. Si le titulaire d'un document électronique décide de ne plus soumettre ses données au prestataire de services de confiance, il avertira ce dernier puis il a droit de retirer le consentement qui lui a été accordé, en lui demandant de détruire et ne plus garder ses données à caractère personnel.

154. La décision de la personne titulaire du document électronique de retirer, voire effacer complètement les données personnelles la concernant, est justifiée par l'un des motifs décrits dans le règlement, tels que l'absence de la nécessité de garder les données ou en cas d'opposition au traitement, ou bien encore en cas de traitement illicites des données[82].

155. Suite à la demande de la personne concernée de l'effacement de ses données personnelles, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend les mesures nécessaires et raisonnables, y compris d'ordre technique, pour l'effacement des données à caractère personnel de la personne concernée (article 7 alinéa 2 du règlement).

[82] Article 17 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), [En ligne : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679].

3) le droit de transférer ses données vers un autre fournisseur de services (droit à la portabilité des données)

156. Lorsque le traitement est effectué via de procédés automatisés, La personne concernée a le droit de recevoir du responsable du traitement les données personnelles la concernant dans un format structuré, couramment utilisé et lisible par machine ; il a aussi le droit de transmettre ces données à un autre responsable du traitement sans que le responsable initial du traitement y fasse obstacle (article 20 alinéa 1er du règlement).

157. En exerçant son droit à la portabilité des données, la personne concernée a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible (article 20 alinéa 2 du règlement).

158. Dans l'hypothèse d'un "document transférable électronique", lorsque la personne titulaire d'un document électronique décide de confier la protection des documents la concernant et ses données à caractère personnel à un autre prestataire de services de confiance, elle exerce son droit à la portabilité des données pour demander à l'ancien fournisseur de transmettre ses données au nouveau responsable du traitement.

4) le droit d'être informé en cas de violation ou piratage des données

159. Lorsqu'il s'agit d'une violation de données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement devra communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais (prévu à article 34 du règlement).

160. La communication de violation de données personnelles doit être effectuée en des termes clairs et simples, pour transmettre la nature de la violation de données à caractère personnel, ainsi que de transmettre les informations suivantes :

i. communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
ii. décrire les conséquences probables de la violation de données à caractère personnel ;
iii. décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

161. Dans la même logique, à partir du moment où le prestataire de services de confiance aperçoit une fuite sécuritaire, il devra immédiatement informer la personne de la violation subies aux documents électroniques la concernant, en lui transmettant les informations citées dessus.

5) Mesures coercitives et pénalités

162. Finalement, la reforme de 2016 a mis en œuvre des mesures coercitives et répréhensibles plus stricte ainsi que des amendes allant jusqu'à 4% du chiffre d'affaires mondial total d'une entreprise, dans le but de décourager la violation des règles. (article 83, 5)). Une telle sanction renforcera la protection des documents électroniques au déprimant du prestataire de services de confiance.

PARAGRAPHE 2 HARMONISATION DES LÉGISLATIONS RELATIVES AUX EFFETS DE COMMERCE INTERNATIONAUX

163. Etant une création de la pratique commerciale et leur attachement aux usages, les effets de commerce trouvent leur origine dans les coutumes marchandes du Moyen Âge.

164. A l'époque du Moyen Age, les marchands développent leurs usages en marge du système féodal ; ceci est pour deux raisons principales : d'une part, le droit canonique se méfie de l'activité commerciale et la considère comme source

de profits illicites et de tentations, et le droit séculier s'élabore autour de la seule vraie richesse, à savoir les immeubles[83].

165. En conséquence, tant que le commerce est un métier inégligeable et qu'il est indispensable pour les marchands de trouver les moyens nécessaires pour pouvoir exercer leur métier malgré la méfiance du droit canonique à leur égard, *"le monde du commerce, manieur de marchandises et d'argent, invente peu à peu son propre droit privé"* [84], ainsi que les outils financiers nécessaires à son activité qui transcendent les frontières des fiefs.

166. Le premier de ces outils à voir le jour est la lettre de change. Celle-ci n'est à l'origine qu'un contrat de change[85] qui sert d'instrument de paiement par lequel les commerçants parcourant les foires à travers l'Europe cherchent à prévenir les risques liés au transport d'argent.

167. Pour limiter les transports de fonds, l'idée était de créer un contrat de change en vertu duquel, le futur acheteur, le bénéficiaire, remet de l'argent à son banquier dans sa propre ville, en échange d'une lettre qui lui permet de recevoir une somme équivalente d'un autre banquier, dans une autre ville et souvent dans une autre monnaie, sous la déduction de la rémunération des banquiers (les agios). Cela supposait que le premier banquier (tireur) avait un correspondant (tiré) dans l'autre ville. La lettre de change s'est ainsi servie comme instrument de transport de fonds[86].

168. Ce n'est qu'à partir du XVIe siècle que la lettre de change se transforme progressivement en instrument de crédit, grâce à l'apparition de la clause à ordre sur le titre au XVIIe siècle, puis à la création de l'escompte en Angleterre et en France au XVIIIe siècle[87].

---

[83] Hilaire, *Introduction historique au droit commercial : PUF, Coll. Droit fondamental, 1986, n° 9*.
[84] Schapira et Leben, *Le droit international des affaires : PUF, 5e éd. 1996, Coll. Que sais-je ?, n° 1465, p. 5*
[85] Hilaire, *op. cit., p. 253, n° 157*.
[86] SZRAMKIEWICZ (R.) et DESCAMPS (O.), *Histoire du droit des affaires*, 22 Octobre 2013, n. 166 s., insiste sur une autre fonction, très tôt apparue aussi : la lettre de change permet de tourner la prohibition du prêt a intérêt, à laquelle se heurte au contraire le billet a ordre. V. aussi, GUEVEL (D.), « L'atomisation du droit cambiaire », *Mélanges P, Simler, Dalloz*, 2006, p. 457 et s.
[87] JEANTIN (M.) et LE CANNU (P.), *Droit commercial, Instruments de paiement et de crédit et entreprises en difficulté : Dalloz, Précis, 5e éd. 1999, n° 226*.

169. Par conséquent, les effets de commerce dispose d'une double fonction car ils servent à la fois en tant qu'instruments de paiement et instruments de crédit. La lettre de change a été utilisée d'abord comme un instrument de paiement, puis progressivement comme instrument de crédit à court terme.

170. Il nous convient d'abord de présenter les caractéristiques de l'effet de commerce en droit interne (I : L'effet de commerce en droit interne), avant de le traiter en droit communautaire et présenter les tentatives de rapprochements des différents systèmes juridiques nationales (*II* : L'effet de commerce en droit international et l'unification des législations en matière de lettres de change).

I. L'EFFET DE COMMERCE EN DROIT INTERNE

A. Notion de l'effet de commerce.

171. Au niveau national, la notion d'effet de commerce ne fait l'objet d'aucune définition précise en droit français. Seuls quelques textes y font allusion, uniquement pour attacher au paiement par effets de commerce des conséquences proches de celles du paiement en numéraire ; nous citerons par exemple dans le texte de l'art. *L. 621-107, 4°*[88] qui a mentionné les effets de commerce parmi les instruments de paiement. Il y a aussi l'article *621-121* du Code de commerce qui fait allusion au terme 'effet de commerce' pour designer les instruments de paiement qui peuvent faire l'objet d'une revendication de la part de vendeurs de meubles pour payer la dette de leurs débiteurs. Nous ajoutons à ces deux derniers articles le texte de l'article *L. 632-1, 4°* du Code de Commerce qui a aussi employé le terme 'effet de commerce' parmi les actes déclarés nuls en cas de redressement judiciaire.

172. Ainsi en raison de l'absence d'une définition légale précise sur l'effet de commerce, il appartient alors à la doctrine de proposer sa propre définition et d'élaborer les classifications indispensables à la description du régime juridique des effets de commerce.

[88] Code de commerce, version consolidée au 20 octobre 2016, [En ligne : https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069565].

173. D'abord, d'après Monsieur le professeur *Delebecque*, l'effet de commerce se trouve défini comme « *un titre négociable qui constate l'existence au profit du porteur d'une créance à court terme et sert à son paiement* »[89]. De cette définition, nous saisissons l'utilisation des termes génériques, ce qui correspond bien à la nature de l'effet de commerce qui comprend divers titres moyens de paiement.

174. Dans une autre tentative à définir l'effet de commerce, Monsieur le professeur Le *CANNU* a présenté l'effet de commerce comme un « *titre négociable et littéral qui représente une créance de somme d'argent stipulée à court terme* [90]». Ici nous reprochons à cette dernière définition le fait qu'il a ajouté le caractère manuscrit des effets de commerce comme condition de formation du titre, ce qui limiterait éventuellement le champs d'application aux seuls documents sous forme manuscrite, en empêchant d'étendre la définition aux documents sous forme électronique.

175. De plus, les Professeur P. *Lescot et R. Roblot*[91] ont proposé de considérer comme effet de commerce, *tout titre, tout écrit reçu couramment en paiement dans les relations commerciales au lieu et à la place de la monnaie, sans présenter pourtant les attributs d'une véritable monnaie. Ce sont des titres négociables, qui portent l'indication de leur valeur, et qui constatent une créance de somme d'argent à court terme*[92].

176. Cette dernière définition montre une autre façade de l'effet de commerce ; il s'agit d'un instrument de financement qui sert à remplacer la monnaie, en constant la somme d'argent faisant l'objet de titre pour une courte durée.

---

[89] Ripert et Roblot par Delebecque et Germain, n° 190.

[90] LE CANNU (P.), GRANIER (T.), ROUTIER (R.), *Instruments de paiement et de crédit Titrisation*, Dalloz, 8ème éd., 2010.

[91] Lescot (P.) et Roblot (R.), *Les effets de commerce : Rousseau 1955, n° 6 s.* ; voir aussi « *Fasc. 2505 : Redressement et Liquidation Judiciaires. – Nullités de droit. – Régime des paiements* », *JurisClasseur Droit international*, 1 Juil. 2001, *LexisNexis SA.*

[92] P. Lescot et R. Roblot, *Les effets de commerce : Sirey*, 1953, *t.* 2 – F. Perochon et R. Bonhomme, *Entreprises en difficulté, Instruments de crédit et de paiement : LGDJ*, 4e éd. 1999, n° 603. – M. Jeantin, *Droit commercial : Dalloz*, 4e éd. 1995, n° 213, p. 126. – Cass. civ., 13 nov. 1889 : S. 1892, 1, p. 437. – CA Bordeaux, 29 mars 1871 : *DP* 1873, 2, p. 213.

B. Traits caractéristiques de l'effet de commerce

177. La notion d'effet de commerce recouvre des divers instruments revêtant d'une double fonction : des instruments de crédit et des instruments de paiement (i.e. la lettre de change, le billet à ordre, le warrant, le chèque.)

178. Nous relevons des définitions doctrinales précédentes que l'effet de commerce s'identifie par la présence de cinq critères essentiels: la négociabilité, un objet monétaire, un engagement de payer, un paiement à court terme et un usage de recevoir le titre en paiement[93]. Ainsi nous présentons les aspects essentiels de l'effet de commerce dans l'ordre suivant:

1) La négociabilité/ transmissibilité des effets de commerce

179. L'un de principaux traits caractéristiques de l'effet de commerce consiste à son aspect négociable. Il s'agit d'un titre négociable, transmissible par l'un des procédés simplifiés de la pratique commerciale ; ce caractère négociable qu'il détient, par dérogation en grande partie aux règles du droit civil, permet une circulation plus rapide, plus simple et plus sûre par rapport au procédé civiliste de cession de créance[94] connu par son coût plus élevé et sa lourdeur, puisqu'il requiert, un acte authentique pour pouvoir produire pleinement ses pleins effets (*C.civ. art. 1690*[95]). Ce procédé est souvent inadapté en droit commercial[96].

180. Quant à la transmission de l'effet de commerce, la circulation du titre s'effectue avec la créance qu'il incorpore par divers moyens, soit par endossement, soit par tradition, s'il est libellé au porteur.

---

[93] GAVALDA (Ch.) - STOUFFLET (J.), *Instrument de paiement et de crédit, LexisNexis - Litec*, 8e éd., 2012.

[94] La cession de créance est définie comme une convention par laquelle le créancier va décider de céder à un tiers, que l'on appelle le cessionnaire à la fois ces droits et ces actions contre le débiteur cédé. Les Obligations entre le cédant et le cessionnaire seront régis par la loi qui s'applique au contrat d'origine entre le créancier cédant et le débiteur cédant. [En ligne: http://www.cours-de-droit.net/la-cession-de-creance-definition-conditions-effets-a121608612].

[95] Article 1690 du Code civil prévoit que « Le cessionnaire n'est saisi à l'égard des tiers que par la signification du transport faite au débiteur. Néanmoins, le cessionnaire peut être également saisi par l'acceptation du transport faite par le débiteur dans un acte authentique ». Ainsi l'exigence d'un acte authentique pour caractériser une cession de créance ; un procédé civiliste jugé lourd et couteux, à l'opposé du procédé simplifié dont il bénéficie l'effet de commerce.

[96] BONHOMME (R.), *Instruments de Crédit et de Paiement*, 10e éd. *L.G.D.J* – 2013, p. 88.

181. D'abord, le moyen le plus simple est la circulation par tradition, qui consiste dans la remise de la main à la main du titre, ce qui suppose un titre au porteur. L'autre procédé qui parait plus efficace et plus sûr que la tradition, est l'endossement ; un procédé qui consiste dans l'apposition au dos du titre d'une signature par le porteur du titre appelé endosseur. Ce procédé suppose un titre à ordre, qui autorise expressément le créancier à se substituer toute personne de son choix sans l'accord du débiteur.

182. Outre les avantages de rapidité et la simplicité dont caractérisent l'effet de commerce, la transmission du titre et de la créance qu'il incorpore est carrément plus efficace que la cession de créance civile. Cette transmission produit des effets supérieurs à ceux de la cession de droit commun, puisque l'endosseur ne se contente pas de garantir l'existence de la créance, mais qu'il en garantit solidairement le paiement par endossement, ce qui assure au nouveau porteur de l'effet de commerce, le porteur, une double protection, par le biais de cette solidarité entre les parties à l'égard de la créance.

183. Autre preuve d'efficacité de l'effet de commerce, c'est l'**autonomie du rapport cambiaire**, tel est le régime applicable aux effets de commerce. Ce principe suppose que le titre vaut par sa seule apparence et se détache de la créance fondamentale, ce qui permet l'incorporation de la créance de somme d'argent dans le titre lui-même. L'incorporation du droit dans le titre, qui cesse ainsi d'être un simple *instrumentum* ; ce qui explique de nombreuses règles du droit cambiaire comme l'indépendance des signatures et l'inopposabilité des exceptions, notamment

184. L'une des règles qui caractérisent le rapport cambiaire est l'**inopposabilité des exceptions.** Cette règle du droit cambiaire signifie que le nouveau titulaire du titre, le porteur, acquiert en principe la créance telle qu'elle résulte apparemment du titre, et donc débarrassée de ses vices, et une sorte de purge s'est ainsi produite afin de protéger le porteur contre tous les moyens de défenses qui auraient pu être opposées au cédant par le débiteur. C'est le

principe de l'*inopposabilité des exceptions* qui sera donc applicable aux effets de commerce[97].

185. Or, la négociabilité influence profondément la nature juridique de l'effet de commerce. Son but consiste à éteindre un rapport juridique préexistant. Dès que l'effet est mis en circulation, il devient abstrait, car le rapport préexistant s'efface ; et de toute façon le nouveau titulaire du titre, le porteur, ne peut pas connaitre ce rapport primaire entre le tireur et le tiré. Ainsi l'effet de commerce se caractérise par cet effet de l'inopposabilité des exceptions.

186. Le principe de l'inopposabilité des exceptions montre aussi l'importance du respect du formalisme en la matière. L'effet de commerce se présente sous la forme d'un titre qui représente le droit au paiement ; il se détache complètement de sa cause initiale de sorte que le porteur est en droit de se fier à la seule apparence de l'effet. Le formalisme est donc imposé, en cette matière, pour la validité du titre. C'est ainsi *le papier qui absorbe l'obligation* »[98].

187. Par ailleurs, pour qu'un titre soit négociable, il faut que ce soit prévu dans la loi et que celle-ci lui reconnaisse ce caractère négociable. Un titre négociable doit aussi contenir une clause de négociabilité (clause à ordre ou au porteur). Ne peut pas être qualifié de négociable un titre incomplet dont le nom de bénéficiaire a été laissé en blanc, à moins que l'usage lui reconnaisse ce caractère ; nous examinons cette hypothèse lorsque nous envisageons plus tard la lettre de change.

188. Comme l'a estimé le Professeur *Schvika*, la dématérialisation des moyens de paiement et de crédit entraine un déclin de la négociabilité[99]. Car d'après lui, le développement de la monnaie scripturale, inscrite dans des comptes qui sont eux-mêmes dématérialisés, a donné naissance à des instruments de circulation

[97] Cette autonomie du régime des effets de commerce conduit a exclure la responsabilité de la banque au titre du devoir de mise en garde ou du respect de la proportionnalité des engagements, à l'égard de l'avaliste : Com. 30 oct. 2012, n° 11-23519, *Bull.* n° 195 ; *Gaz. Pal.*, 12 déc. 2012, chron. 12, n. Dumont-Lefrand ; *Banque et Dr*. Nov. 2012. 54, n. Jacob ; *RLDA* déc. 2012. 30, n. Mauriès ; *RTD com.* 2013. 124, obs. Legeais.

[98] Roblot. Ibid. n° 88.

[99] Schvika, *Du déclin de la négociabilité des instruments de paiement et de crédit* : *D.* 2000, *chron*, p. 615.

de la monnaie qui ne reposent pas sur la négociation d'un titre (i.e. les cartes de paiement, les transferts électroniques de fonds…). Nous évoquons par cette opinion la crainte et la méfiance à l'égard de la nouvelle technologie et les nouvelles techniques commerciales : ces dernières ne seront pas capables de produire un effet de commerce négociable, équivalent à celui sous forme manuscrite. Une telle crainte que nous démontrerons, au fur et à mesure de notre étude, est injustifiée en présence d'un système juridique régissant les instruments de paiement et le crédit électroniques.

2) Objet monétaire

189. L'importance de l'élément formel s'explique par le fait que l'effet de commerce ne constate pas seulement un engagement commercial. Il joue aussi le rôle de monnaie. Le titre ne peut équivaloir à la monnaie que s'il a un objet monétaire, c'est-à-dire s'il constate le droit à la remise d'une somme d'argent, et si le montant en est exprimé, ce qui est caractérisé en matière d'effet de commerce.

3) Engagement de payer

190. L'effet de commerce est caractérisé par l'engagement de payer une somme d'argent souscrit par l'émetteur ; et qu'une simple cession de créance au porteur ou à ordre ne répond pas à cette condition si le cédant n'en garantit pas le règlement à tout porteur[100].

4) Un engagement à court terme

191. L'effet représente une somme d'argent déterminée payable à court terme, ce qui explique son statut de crédit à court terme. Ainsi, un titre négociable et littéral ne pourra être considéré comme un effet de commerce que lorsqu'il constate une créance a court terme. La fixation d'une date limite précise est pourtant difficile à déterminer dans la plupart des cas[101]. Nous laissons ainsi à la

[100] STOUFFLET (J.), *Op. Cit.* p. 13.

[101] '*On indiquera seulement que si elle fournit un ordre de grandeur, la limite de quatre-vingt-dix jours que la Banque de France fixe en principe pour l'escompte commercial n'est pas à retenir comme critère. Une*

doctrine et aux usages commerciaux le soin de déterminer le terme et la date d'exigibilité d'un effet de commerce.

5) Usage de recevoir le titre en paiement

192. L'effet de commerce a fait son grand succès à l'époque du Moyen Âge en l'utilisant en tant qu'instrument de paiement pour remplacer l'argent, en offrant aux commerçants un moyen plus sécurisé pour conclure leurs transactions, bien qu'en droit les effets de commerce sont présentés comme des instrument de crédit à court terme.

193. Nous tenons ainsi compte de la pratique qui reconnait aux effets de commerce un pouvoir libératoire (même s'ils ne l'ont pas en droit) ou les considère comme de la quasi-monnaie grâce aux facilités de mobilisation qu'ils comportent, tandis que d'autres titres sont écartés de tels emplois bien que leurs caractéristiques objectives ne les en excluent pas.

II. L'EFFET DE COMMERCE EN DROIT INTERNATIONAL ET L'UNIFICATION DES LÉGISLATIONS EN MATIÈRE DE LETTRES DE CHANGE

194. Lorsque les États se constituent sous leur forme moderne unitaire, ils ne laissent plus aux commerçants le soin de gérer leur métier et leur droit professionnel. Les États créent leurs propres règles juridiques afin de gouverner la vie professionnelle des marchands et réglementent les effets de commerce, soit en les fondant dans un droit commun, comme la *common law* britannique, soit en, en créant un droit spécifique, à l'instar de l'État français[102].

195. Ainsi les droits étatiques ont confisqué le droit unique des marchands en formant par leur diversité une pluralité de systèmes juridiques étatiques dont la

---

date d'exigibilité sensiblement plus éloignée n'est pas exclusive de l'appartenance à la catégorie des effets de commerce'. STOUFFLET (J.), Instrument de paiement et de crédit, Ibid.

[102] Schapira et Leben, *Le droit international des affaires : PUF, 5e éd. 1996, Coll. Que sais-je ?, n° 1465, p. 6.*

vocation à régir les effets de commerce internationaux produit des situations conflictuelles ;ainsi le droit uniforme des marchands cède le pas et ne mettra pas fin aux conflits de lois[103].

196. Au XIXe siècle les divergences entre les droits étatiques en Europe s'accentuent lorsque les juristes allemands faisaient de la lettre de change un titre formel, émancipé des motifs pour lesquels le tireur l'a souscrite, et qu'ils adoptent leur propre droit positif distinct par le biais de la *Conférence de Leipzig* de l'ordonnance de 1848 servant à unifier les législations des États allemands[104]. L'Europe occidentale du XIXe siècle connaît alors trois principaux types de droits susceptibles de régir les effets de commerce: le droit issu de la *common law*, le droit commercial de tradition latine et le droit allemand.

197. Ainsi apparut la nécessité d'harmoniser les législations cambiaires ; une quête de règles uniformes a débuté en 1850 et a abouti, le 7 juin 1930, à l'adoption sous l'égide de la Société des Nations à Genève de deux conventions complémentaires, la première portant *"loi uniforme sur les lettres de change et billets à ordre"*, la seconde étant destinée à régler certains conflits de lois relatifs à ces mêmes effets de commerce[105].

198. Nous retenons ici deux remarques: d'une part, bien que les Conventions de Genève aient servi à unifier les législations de nombreux pays européens, leur adoption a également consommé la rupture entre les droits continentaux et les droits anglo-saxons : la Grande-Bretagne et son empire, ainsi que les États-Unis ont conservé leur droit fondé sur le *Bill of Exchange Act*[106], texte de 1882 codifiant la coutume anglaise[107] qui, au XIXe siècle, s'est affranchie de

---

[103] HUON (PH.), *Droit Uniforme en Droit du Commerce International*, [En ligne : http://www.memoireonline.com/01/08/866/m_droit-uniforme-droit-commerce-international4.html].
[104] *Hilaire, op. cit., n° 183.*
[105] Sur l'historique de cette période, *V.* Bayalovitch, *Le droit international du change : thèse, Lyon, 1935, n° 62 à 78.* - Arminjon et Carry, *La lettre de change et le billet à ordre : Dalloz, 1938, n° 10 à 13.* - Loussouarn et Bredin, *Droit du commerce international : Sirey, 1969, n° 444.* - Roblot, *Les effets de commerce : Sirey, 1975, n° 49.*
[106] *Bill of Exchange Act 1882* [En ligne: http://www.legislation.gov.uk/ukpga/Vict/45-46/61].
[107] Loussouarn et Bredin, *Droit du commerce international : Sirey, 1969, n° 444.* - Roblot, *Les effets de commerce : Sirey, 1975, n° 445.*

l'influence du droit français et des théories de Pothier[108]. Depuis lors, les systèmes anglo-saxon et continental s'opposent sur de nombreux points.

199. D'autre part, les deux Conventions de Genève présentent un certain nombre d'insuffisances qui rendent leur importance pratique moins significative. Elles n'ont donc pas mis fin aux velléités unificatrices des organisations internationales. C'est ainsi que la Commission des Nations unies pour le Droit commercial international (*CNUDCI*) a élaboré une Convention *"sur les lettres de change internationales et les billets à ordre internationaux"*, adoptée par l'Assemblée générale des Nations unies le 9 décembre 1988[109]. Ce texte ambitieux tente de résoudre le clivage entre le droit continental et le droit anglo-saxon en créant une lettre de change et un billet à ordre internationaux et en leur appliquant des règles communes aux deux systèmes lorsque cela est possible ou, lorsqu'il y a des conflits, en proposant soit des solutions de compromis, soit des règles novatrices.

200. Malgré la diversité des législations nationales[110] et du droit conventionnel, l'origine internationale des effets de commerce confèrent à ces derniers une ressemblance certaine, tant en ce qui concerne leur rôle que leur régime juridique. Pourtant il ne faut pas en déduire que le concept d'effet de commerce est unitaire et harmonieux dans l'ensemble des législations.

201. En effet, les difficultés que le législateur français a rencontré en droit interne sont accrues en droit du commerce international. Ainsi, les droits américain, italien, allemand ou suisse retiennent une notion d'effet de commerce plus extensive que celle adoptée par la doctrine française et utilisent des critères discriminants différents : alors que le critère de l'incorporation prévaut en Allemagne, en Suisse *("Wertpapiere")* et en Italie *("titulo di credito")*, la théorie

[108] *Arminjon et Carry, op. cit., n° 143 s.*
[109] Convention des Nations Unies sur les lettres de change internationales et les billets à ordre internationaux (*New York*, 1988), [En ligne : http://www.uncitral.org/uncitral/fr/uncitral_texts/payments/1988Convention_bills_promissory.html].
[110] *V.* pour un exemple, Al Bejad, *Les lettres de change dans les relations internationales : étude comparative des droits cambiaires français et des États du Conseil de coopération des États arabes du Golfe : thèse, Rennes 1, 1993.*

anglo-saxonne de la négociabilité l'emporte aux États-Unis *(UCC, art. 3)* [111]. Il en résulte par exemple que les *"negotiable instruments"* anglo-saxons recouvrent classiquement la lettre de change, le billet à ordre, le chèque, les billets de banque, les bons du Trésor... [112]. Comparée à la stricte énumération du Code de commerce français, énumérer cette liste montre clairement l'absence d'unité de la notion d'effet de commerce dans les législations nationales.

202. Ainsi il est devenu urgent de trouver une notion unitaire d'effet de commerce ; Les professeurs Chaput et Schödermeier avaient estimé cette exigence pour deux raisons principales[113] :

- d'une part, une notion unitaire qui permettrait à la doctrine à dégager un régime commun des effets de commerce ;
- d'autre part, elle permettrait d'évaluer avec précision la portée des textes qui font expressément référence aux effets de commerce (par exemple, *C. com., art. L. 621-107 et L. 621-121. - Adde* plus récemment, *C. com., art. L. 441-7*).

203. Pour autant, bien que les effets de commerce n'aient pas les mêmes statuts juridiques au niveau national, les lois nationales confèrent aux effets un régime spécifique complet, ce qui ne rend pas indispensable l'application d'une notion unitaire, comme l'ont estimé les professeurs Chaput et Schödermeier ; et ce sera conformément à un principe bien établi, le juge saisi d'une difficulté de qualification d'un titre opérera selon les conceptions de la loi du for[114].

204. Les moyens utilisés pour unifier le régime des lettres de change et des billets à ordre sont de natures très variées. D'abord, par le biais des conventions de Genève en 1930; ces dernières avaient tenté d'agir sur les législations nationales et afin de combler les lacunes laissées par les désaccords relatifs à certaines questions de droit matériel sur les règles de conflit de lois (A). La CNUDCI a fait un travail très audacieux visant à la création d'une nouvelle

---

[111] *U.C.C.* – Article 3 – *Negotiable Instruments* (2002), *Uniform Commercial Code*, [En ligne : https://www.law.cornell.edu/ucc/3**].**

[112] Ripert et Roblot, *Traité de droit commercial : LGDJ,* 16e éd. *2000, t. 2, par Delebecque et Germain, n° 1912.*

[113] CHAPUT (Y.) et SCHODERMEIER (M.D.), *Effets de commerce, chèques et instruments de paiement : PUF, Coll. Droit fondamental, 2e éd. 1998, n° 3.*

[114] Roblot, *Les effets de commerce : Sirey, 1975, n° 657.* - Batiffol et Lagarde, *Traité élémentaire de droit international privé : LGDJ, 8e éd. 1993, t. 1, n° 292.*

catégorie d'instruments de crédit : la lettre de change international le et le billet à ordre international (B).

A. Les mouvements d'unification avant l'arrivée de la CNUDCI

205. Le premier mouvement signifiant de l'unification internationale du droit des effets de commerce, aussi bien au niveau des règles de fond que celles de conflits de lois, remonte aux deux conférences de La Haye de juin 1910 et juin 1912. La seconde de ces conférences avait adopté, en juillet 1912, un règlement uniforme relatif à la lettre de change et au billet à ordre. L'année 1912 marque la date de naissance de la Convention introduisant un règlement uniforme sur les lettres de changes et les billets à ordre. Celle-ci est signée par 17 pays européen et 10 autres provenant de l'Amérique centrale et l'Amérique du Sud.

206. Interrompu par la première guerre mondiale, ce travail d'unification fut repris, sous l'égide de la Société des Nations, des 1920 ; en 1927, un pas décisif fut franchi par la convocation d'une commission d'experts dont les travaux furent soumis à la conférence internationale de Genève de mai - juin 1930. Cette conférence adopta, le 7 juin 1930, six conventions : trois sur le chèque et trois sur la lettre de change et le billet à ordre. La première de ces trois conventions visait l'unification des règles de fond internes : il s'agit d'une loi uniforme que les signataires de la convention s'engagent à intégrer dans leur ordre juridique interne. La deuxième convention a trait au règlement uniforme des conflits de lois en matière de la lettre de change. La troisième concerne les droits de timbre.

207. Le travail effectué à La Haye, servant d'assise aux travaux de la Société des Nations lors de la Conférence internationale pour l'unification des lois relatives aux lettres de change, billets à ordre et chèques tenue à Genève en 1930 a abouti à la naissance de Convention de Genève portant Loi uniforme (ci-après Convention LU).

208. La Convention LU contient en première annexe les soixante dix-huit articles qui fixent le régime de la lettre de change et du billet à ordre, intégrés depuis le décret-loi de 1935 dans le Code de commerce français *(C. com., art. L.*

511-1 s.); puis la deuxième annexe comporte vingt-trois articles assortis de certaines réserves, autorisant les États signataires à déroger à la Convention sur des éléments spécifiques[115].

209. Cet ensemble de textes constitue le socle du progrès législatif dont nous témoignons aujourd'hui[116]. Pourtant bien que la Convention LU ait achevé un degré considérable d'harmonisation, elle ne réussit toutefois pas à rallier les pays anglo-saxons. Elle n'est pas non plus exempte de critiques eu égard à sa vocation universelle. Nous reprochons à ces règles les déficiences présentées dans l'ordre suivant[117] :

- **Restrictions à l'uniformisation dans l'espace :**

210. En premier lieu, cette œuvre n'a pas réussi à réduire l'opposition existante entre les pays de *common law* et les pays de droit civil : ceci est dû principalement au refus des pays anglo-saxons d'adhérer à la loi uniforme en reposant sur des considérations juridiques, politiques et historiques. En fait, les Etats Unis et l'Angleterre avaient déjà manifesté leurs réticences à modifier leur législation.

211. Nous expliquons le refus des pays anglo-saxons à l'adhésion à la loi uniforme par le fait que juridiquement, le droit cambiaire anglo-saxon présente certaines particularités par rapport au système issu du droit uniforme:

- tout d'abord, la différence majeure et la plus remarquable entre les deux systèmes, c'est que le droit anglo-saxon est un système juridique exempt de formalisme[118] : aucune mention obligatoire n'est imposée par la loi, ni à l'émission, ni lors des transmissions du titre; c'est le contexte et l'analyse des

[115] Les Etats Parties s'engagent à introduire dans leurs territoires respectifs la Loi uniforme formant l'Annexe I de la Convention de Genève. Pourtant cet engagement sera éventuellement subordonné aux réserves que chaque Etat membre devra, dans ce cas, signaler au moment de sa ratification ou de son adhésion. Ces réserves sont mentionnées à l'Annexe II de la Convention LU qui contient 23 articles, [En ligne : https://www.admin.ch/opc/fr/classified-compilation/19310012/index.html].

[116] Bayalovitch, *Le droit international du change : thèse, Lyon, 1935, n° 62 à 78. - Arminjon et Carry.*

[117] Vincent Thomas, *Fasc. 566-20 : Effets de commerce. - Lettre de change et billet à ordre. – Warrant, JCP 30 Oct. 2002, n° 14.*

[118] Bloch, *Les lettres de change et billets à ordre dans les relations commerciales internationales, Étude comparative de droit cambiaire français et américain : Economica, 1986, n° 146.* - Mattout, *Droit bancaire international : Banque, 2e éd. 1996, n° 40.* - Coutenier, *Les techniques de mobilisation des créances internationales, Aspects de droit international et de droit comparé : RD aff. int. 3/1999, p. 295 s., spéc. n° 4 s, n° 74.*

circonstances de chaque document qui permet de différencier la lettre de change *("bill of exchange")* du billet à ordre *("promissory note")*, alors que la loi uniforme, comme le droit français, consacre la conception scripturale formelle allemande de ces deux effets de commerce[119];

- ensuite, lorsque nous envisageons l'hypothèse d'une fraude en droit anglo-saxon, le porteur de l'effet a un statut précaire dans la mesure où la signature contrefaite est dénuée de tout effet : celui qui a apposé une fausse signature n'acquiert pas de droit et ne peut davantage en transmettre aux endossataires ultérieurs ; il en résulte que pour ces derniers l'impossibilité de se retourner contre les signataires antérieurs au faussaire ; or d'après le système anglo-saxon, la régularité apparente de la chaîne des endossements ne permet pas de légitimer les droits du détenteur de l'effet de commerce en cas de contrefaçon[120], contrairement à la solution retenue en droit français, par exemple, où l'*article L. 511-11 du Code de commerce* se contente d'une "légitimité formelle"[121] pour procurer une protection découlant de la nature cambiaire du titre;

- enfin, la bonne foi du porteur est conçue différemment dans les deux systèmes : alors qu'elle est acquise en droit anglo-saxon au porteur qui ignorait, au moment de la négociation, le vice affectant le titre, le porteur est de bonne foi selon la loi uniforme à moins qu'il *"n'ait agi sciemment au détriment du débiteur"(Conv. LU, annexe I, art. 17. - C. com., art. L. 511-12)* ; interprétant cette expression, la jurisprudence française creuse le fossé qui sépare notre droit du système de *common law* en exigeant que le porteur ait eu conscience du préjudice que l'endossement cause au débiteur de l'effet par l'impossibilité où il le met de se prévaloir, vis-à-vis du tireur ou d'un précédent endosseur, d'un moyen de défense issu de ses relations avec ces derniers[122] .

---

[119] *Conv. LU, annexe I, art. 1 et 2. - Adde, C. com. fr., art. L. 511-1. - C. civ. suisse, art. 991 et 992.*

[120] *BEA, section 24. - UCC, art. 3-404, 3-405, 3-603. - Bloch, Les lettres de change..., op. cit., n° 240. - Pinault, La réconciliation des irréconciliables : la Convention des Nations unies sur les lettres de change internationales et les billets à ordre internationaux : Les Cahiers de Droit, Université Laval [Québec], vol. 38, n° 3, sept. 1997, p. 533 et 534.*

[121] Cabrillac, *cité par Gavalda et Stoufflet, op. cit., n° 46.*

[122] *Cass. com., 26 juin 1956 : JCP 1956, II, 9600, note Roblot ; RTD com. 1957, p. 147,* obs. Becqué et Cabrillac. - *13 janv. 1987 : Bull. civ. IV, n° 17 ; RTD com. 1988, p. 469,* obs. Cabrillac et Teyssié. - *11 juill. 2000 : RJDA 12/2000, n° 1164.* - Gavalda et Stoufflet, *op. cit., n° 55-1 s.*

212. Ces différences majeures existant entre les deux systèmes constituaient un obstacle à l'adhésion des pays de *common law* à la convention de La Haye. D'autres raisons d'ordre politique et historique ont mené à accentuer l'écart entre les deux systèmes juridiques. En effet, Il n'était pas évident pour les pays appartenant à la communauté anglo-saxonne de pouvoir adhérer à la Convention de Genève.

213. Bien que les Etats Unis et l'Angleterre aient participé à l'ensemble des conférences de La Haye, ces deux pays avaient clairement établi qu'ils n'entendaient pas apporter de modifications à leur législation relative aux effets de commerce quels que soient les résultats obtenus à la conférence.

214. Cette position pour l'Angleterre se justifiait par le fait que les pays de *common law* avaient déjà procédé entre eux à une certaine uniformisation à partir de la fin du XIXe siècle ; tout a commencé par une coutume établie par les pratiques du milieu bancaire ; le *Bill of Exchange Act*[123]*en 1882* qui a connu un grand succès et qu'il a par la suite influencé les pays faisant parties de l'Ancien Empire britannique à l'époque. Parmi ces pays qui avaient adhéré à la convention le Canada, les Indes ou l'Australie dès la fin du XIXe siècle.

215. Ne servant pas seulement de base à la législation de la plupart des pays du *common wealth*, cette convention avait aussi servi les États-Unis qui l'avaient prise pour modèle afin d'élaborer leur propre loi uniforme sur les effets de commerce en 1986[124] (*"Negotiable Instruments Act"* de 1896), adopté par les États de l'Union de 1897 à 1927[125]*).*

216. Les pays faisant partie de la communauté anglo-saxonne et soumis à l'influence du *Bill of Exchange Act* n'avaient pas un vrai intérêt à adopter la Convention de Genève, et de faire éclater l'unification qu'ils espèrent réaliser. Ils n'étaient donc pas disposés à sacrifier les résultats atteints par cette dernière

[123] *Ibid* p. 51.
[124] Bayalovitch, *Le droit international du change : thèse, Lyon, 1935, p. 60, note 23.*
[125] *"Negotiable Instruments Act"* de 1896, adopté par les États de l'Union de 1897 à 1927; *Uniform Negotiable Instruments Act Drafted by the National Conference of Commissioners on Uniform State Laws, and by it Approved and Recommended for Enactment in All the States at Its Conference at Saratoga Springs, N.Y.*, August 15-18, 1896.

unification. Ainsi l'intérêt de la Convention LU est devenu moins significatif, voire même très faible, pour ces États.

217. D'autre coté, nous nous rendons compte de la réticence de certains États d'Amérique latine, puisqu'il ne s'agit que seulement quatre États sud américains qui avaient signé la Convention sur la Loi Uniforme : la Colombie, l'Équateur, le Pérou et le Brésil ; et seul ce dernier la ratifia. Ce manque de succès de la Convention dans ces pays d'Amérique latine s'explique par le fait que ces pays sont trop influencés par le droit anglo-saxon.

218. D'ailleurs, ce manque de succès de la Convention de Genève dans les pays d'Amérique latine résulte aussi du fait que ces derniers espéraient davantage de l'unification des règles de rattachement que de l'harmonisation des droits internes. C'est ainsi que quelques années plus tard l'Organisation des États américains a adopté une convention interaméricaine sur les conflits de lois concernant les lettres de change, billets à ordre et factures, signée en 1975 et ratifiée à ce jour par quatorze États, dont l'Argentine, le Chili, le Mexique, le Pérou, l'Uruguay et le Venezuela.[126]

- **Uniformisation limitée du droit matériel**

219. En deuxième lieu, la Convention LU de Genève ne réalise pas une unification complète du droit matériel applicable aux effets de commerce. En fait, l'une des raisons qui avaient participé au succès relatif de la Convention LU est son incapacité à complètement unifier les droits internes. Par peur de faire échouer leur initiative, les parties à la convention avaient délibérément fait l'impasse sur certains points présentés comme lacunes de droit, en renvoyant de nombreuses questions à la compétence de leurs législations internes et ainsi d'aménager de multiples réserves.

220. Citant un exemple de renvoi à la compétence de législation interne, permettant de maintenir intact le système de la loi française, en prévoyant que *"la question de savoir si le tireur est obligé de fournir provision à l'échéance et*

[126] Le texte de la convention et la liste complète des États signataires et ayant ratifié sur www.oas.org.

*si le porteur a des droits spéciaux sur cette provision reste en dehors de la loi uniforme" (*article 16, alinéa 1er de l'annexe II[127]*).* Ce texte, ajouté à la demande de la France, préserve les systèmes juridiques qui organisent la transmission de la provision avec l'émission et l'endossement de l'effet, comme les systèmes français, belge ou luxembourgeois, et limite l'influence du système allemand qui confère à l'obligation cambiaire un caractère exclusivement littéral[128].

221. A propos de réserves, il y en a vingt-trois articles de l'annexe II de la Convention LU qui mentionnent les réserves que les États contractants pouvaient choisir au moment de la ratification ou, pour certaines d'entre elles *(art. 8, 12 et 18),* postérieurement à la ratification ou à l'adhésion ou encore, pour d'autres *(art. 7 et 22),* à tout moment. Ainsi les États qui ont accepté de ratifier la Convention de Genève ont largement usé du recours aux réserves. Comme le cas du Japon, les Pays-Bas et l'ex-URSS ont donné ratification de la loi uniforme sous réserve du bénéfice de toutes les dispositions figurant à l'annexe II.

B. Uniformisation des instruments de crédit : Convention CNUDCI

1) Création d'effets internationaux par la CNUDCI

222. Les acteurs du troisième mouvement à l'uniformisation des instruments de crédit ont pris conscience de l'échec des Conventions de Genève : puisque les deux textes des Conventions de Genève n'ont pas réussi à unifier ni les législations nationales, ni les règles de conflits de lois ; l'idée donc a été relancée d'unifier les instruments eux-mêmes en créant des effets dotés d'un régime propre combinant les systèmes continental et anglo-saxon. C'est la CNUDCI qui a pris la relève en multipliant les travaux d'unification en1971[129]. Conformément à la méthode de travail de la CNUDCI, un groupe de travail formé d'experts sur

[127] Annexe II de la Loi uniforme sur les lettres de change et billets à ordre, conclue à Genève le 7 juin 1930, [En ligne : https://www.admin.ch/opc/fr/classified-compilation/19300022/200508170000/0.221.554.1.pdf]. . Voir aussi la note à l'art. 54 al. 6 de la loi uniforme.

[128] Coutenier, *Les techniques de mobilisation des créances internationales, Aspects de droit international et de droit comparé : RD aff. int. 3/1999, p. 295 s., spéc. n° 8.*

[129] *V. Commentaires de la CNUDCI sur les projets de convention : Annuaire CNUDCI, Vol. III, 1972, p. 145, A/CN. 9/67 ; Annuaire CNDUCI, Vol. XIII, 1982, p. 71, A/CN. 9/211.* - Adde Roblot, *Une tentative d'unification mondiale du droit : le projet de la CNUDCI pour la création d'une lettre de change internationale,* Études offertes à Jean Vincent *: Dalloz 1981, p. 361.* - Bloch, *Le projet de convention sur les lettres de change internationales et les billets à ordre internationaux : JDI 1979, p. 770.*

le sujet provenant de plus de 50 pays est institué en Avril de l'année 1971 et qui aboutit la rédaction du premier projet en 1972, suivi d'une rédaction finale en 1981. Quelques années plus tard, les efforts du groupe de travail de la CNUDCI ont abouti à l'adoption par l'Assemblée générale des Nations unies d'une convention sur les lettres de change internationales et les billets à ordre internationaux le 9 décembre 1988[130].

2) <u>Champ d'application de la convention.</u>

223. La CNUDCI a exclu de son champ d'application le chèque international de son projet ; et la convention ne s'applique qu'aux lettres de change internationales et aux billets à ordre internationaux comportant dans leur en-tête et dans leur texte les termes "Lettre de change internationale" ou "Billet à ordre international" *(Conv. CNUDCI, art. 1).*

224. Le recours à ces "instruments CNUDCI" est facultatif et donc laissé à la discrétion de leurs utilisateurs. Cela signifie qu'un État partie à la Convention ne pouvait soumettre impérativement les effets internationaux émis sur son territoire au régime juridique établi par ladite Convention.

225. Aux termes du texte de l'*article 3 de la Convention CNUDCI*, deux (2) définitions ont été élaborées pour les instruments la régissant. D'abord, la lettre de change internationale est décrite comme un instrument écrit qui :

- *contient le mandat inconditionnel donné par le tireur au tiré de payer une somme déterminée au bénéficiaire ou à son ordre ;*
- *est payable à vue ou à une échéance déterminée ;*
- *est daté ;*
- *est signé par le tireur.*

226. De l'autre côté, Le billet à ordre international est définit comme un instrument écrit qui :

- *contient l'engagement inconditionnel pris par le souscripteur de payer une somme déterminée au bénéficiaire ou à son ordre ;*

[130] Convention et note du Secrétariat de la CNUDCI sur *www.uncitral.org*. - Support papier de la note du Secrétariat de la CNUDCI : *Annuaire CNUDCI, vol. XXV, 1994, p. 265, A/CN. 9/386.*

- *est payable à vue ou à une échéance déterminée ;*
- *est daté ;*
- *est signé par le souscripteur.*

227. Sur le caractère international de l'effet de commerce, les études effectuées par la CNUDCI ont démontré que plusieurs Etats ne sont pas prêts à remplacer leur législation nationale établie par de nouvelles règles uniformes. Donner satisfaction à ces Etats est effectivement possible par la création d'un nouvel effet de commerce et la convention CNUDCI prévoit que l'effet de commerce doit avoir un caractère international pour qu'elle s'applique à celui-ci.

228. D'après la Convention CNUDCI, une lettre de change internationale doit désigner au moins deux des lieux indiqués sur la lettre ou le billet; ces lieux devant être situés dans des États différents. Ce sont le lieu où la lettre est tirée, le lieu désigné à côté de la signature du tireur, du nom du tiré ou du nom du bénéficiaire, le lieu du paiement.

229. Nous retenons ici que la Convention CNUDCI confère une importance toute particulière au lieu où la lettre est tirée et au lieu du paiement de la lettre et du billet parce que c'est grâce au lieu de l'émission du titre que l'aspect international du titre sera caractérisé.

230. Ainsi selon l'instrument concerné, l'un de ces lieux au moins doit être précisé sur le titre et doit se situer dans un État contractant. À défaut, l'instrument n'est pas considéré comme un effet international au sens de la Convention CNUDCI.

231. **Pour conclure,** la Convention CNUDCI est présentée comme un outil assez séduisant pour les praticiens en raison de la souplesse de son utilisation, de son caractère non contraignant ; et bien que d'importantes dispositions de la Convention relèvent essentiellement de règles issues de la *common law*, il n'en demeure pas moins que les principes provenant du droit civil y ont été maintes

fois consacrés, notamment par l'exigence d'un certain formalisme et par l'admission assez large de l'inopposabilité des exceptions[131].

232. Certains titres négociables répondent aux critères précités sur les effets de commerce. C'est le cas, en tout premier lieu, de la lettre de change, l'écrit par lequel un tireur invite un tiré à verser une somme d'argent à l'ordre d'un preneur ou bénéficiaire, à une date déterminée et s'oblige à payer si le tiré ne le fait pas.

233. Est également qualifié d'effet de commerce le billet à ordre, écrit par lequel un souscripteur s'oblige à payer une somme d'argent à l'ordre d'un preneur ou bénéficiaire, à une date déterminée et s'oblige à payer si le tiré ne le fait pas. La même qualification s'impose pour le warrant qui s'analyse en un billet à ordre garanti par un gage sur des marchandises déposées, en principe, dans un magasin public.

234. Afin d'encadrer les titres faisant l'objet de la présente recherche, parmi les différentes catégories des effets nous pouvons envisager un DTE sur une lettre de change et un billet à ordre et un warrant-gage. Pourtant le cheque a été exclu pour les raisons précédemment présentées dans l'introduction.

235. **Conclusion intermédiaire –** La connaissance et l'organisation et ces textes relatifs aux instruments de paiements étaient nécessaires, car c'est par rapport au respect de conditions spécifiques de forme et de fond de l'effet de commerce sous forme manuscrite que va être apprécié .la validité et la conformité du *'document transférable électronique'*

[131] Vincent Thomas, *Op. Cit., p.16, n°50.*

SECTION II

CONDITIONS DE VALIDITÉ DES ‘DOCUMENTS TRANSFÉRABLES ÉLECTRONIQUES’

236. Les ‘documents transférables électroniques’ (ci-après ‘DTE’) ont des caractéristiques qui les rapprochent de leurs équivalents sous forme manuscrite, bien qu’il y ait d’autres aspects qui les démarquent de ces derniers. L’intérêt de la présente section est d’introduire le DTE, par le biais de la présentation de conditions de formation et de validité de cet instrument sous deux aspects : manuscrite et informatisée électronique.

237. Un DTE n’est en réalité qu’un effet de commerce revêtant une forme électronique pour répondre à l’évolution des techniques commerciales; il est ainsi possible de présenter les aspects communs entre ces deux instruments avant de dévoiler leurs points de divergence.

238. Bien qu’un DTE soit l’équivalent électronique d’un effet de commerce, ce dernier est plus connu par son statut formaliste, sa forme manuscrite et son caractère négociable, rendant la reconnaissance de l’équivalent électronique plus difficile à accepter sur le plan juridique ; c’est la raison pour laquelle un DTE s’est présenté pendant ces deux dernières décennies comme un nouveau défi à relever en droit du commerce international.

239. Alors lorsque nous traitons les exigences de forme pour valider un document transférable électronique, on revient, par respect du principe de parallélisme de forme, aux critères de base de leurs équivalents sous forme manuscrite ; et qu’à partir de là que nous identifierons les éventuelles différences entre ces deux formes de documents.

240. Parlons des lettres de change et billet à ordre, ces instruments sont des formes variées d'un titre qui est l'effet de commerce. Dans cette deuxième et dernière section du chapitre consacré aux conditions de validité, la distinction fondamentale se porte sur l'instrument financier transférable et le document 'formant titre'. Le premier représente une somme d'argent - tel est le cas de la lettre de change et le billet à ordre - (*paragraphe 1 : instruments financiers de mobilisation de créance – les lettres de change et les billets à ordre*) alors que le second représente des marchandises comme les warrants et les récépissés d'entrepôt (*paragraphe 2 : instruments financiers de garantie de créance – warrants et les récépissés d'entrepôt*).

PARAGRAPHE I. INSTRUMENTS FINANCIERS DE MOBILISATION DE CRÉANCE
LES LETTRES DE CHANGE ET LES BILLETS À ORDRE
(« LES INSTRUMENTS TRANSFÉRABLES »)

I. FORMATION DE LA LETTRE DE CHANGE

A. Présentation générale de la lettre de change.

1) Notion de la lettre de change.

241. Etant réputée comme l'archétype de l'effet de commerce, dotée d'un statut juridique complet, la lettre de change qui, selon la définition la plus couramment admise, est un titre par lequel une personne (le tireur) donne à une autre (le tiré) l'ordre de payer à une tierce personne (le bénéficiaire) ou à son ordre une certaine somme à une époque déterminée.

242. Il s'agit d'un titre négociable qui constate l'existence au profit du porteur d'une créance à court terme et sert à son paiement. La lettre de change est remise par le tireur au bénéficiaire, à qui est conféré ces droits, mais naturellement, le tireur est tenu de payer la lettre de change si le tiré ne le fait pas.

243. Historiquement, la lettre de change, portant bien souvent en pratique le nom de 'traite', est l'un des instruments de paiement et de crédit à court terme les plus anciens lorsqu'il apparait la première fois à l'époque du Moyen Age, et est pratiqué dans les foires comme un moyen de paiement entre commerçants.

244. La lettre de change apparait au Moyen Age sur la base d'un contrat particulier appelé 'contrat de change'. Celui-ci est défini comme « *la convention par laquelle le donneur fournissait une somme d'argent au preneur et recevait en échange un engagement payable à terme mais en un autre lieu et une autre monnaie* »[132]. Nous retenons de cette définition que la lettre de change est une manifestation d'un rapport triangulaire où le tiré est débiteur du tireur qui est le rapport fondamental, et le tireur, débiteur du bénéficiaire.

245. Le législateur français a attribué à la lettre de change le caractère commercial dans le texte de l'*article 110-1.10°*, il s'agit d'un acte commercial par la forme[133], et relève donc de la compétence des tribunaux de commerce (*C. org. Jud., art. L.411-4*[134]).

246. Etant un acte juridique, la lettre de change est soumise aux conditions du droit commun des actes juridiques. Mais en tant qu'acte de commerce, elle présente une certaine spécificité qui se manifeste à trois points de vue. Il s'agit là de trois rapports juridiques distincts qui pourront avoir lieu lorsque nous envisageons une lettre de change dans une opération commerciale :

- Rapport fondamental entre le tireur et le tiré ;
- Rapport entre le tireur et sa banque ;

---

[132] Définition rapportée par HILAIRE (J.), *Introduction historique au droit commercial* : PUF, *Coll. Droit fondamental*, 1986, p.255. *Comp*. Avec la définition donnée par R.J/Pothier (traité du contrat de change, Debure, 1773, p.2) « *un contrat par lequel je vous donne ou m'engage à vous donner une certaine somme en un certain lieu pour et en échange d'une somme d'argent que vous obligez de me faire compte en un autre lieu* ». On perçoit aisément l'élément essentiel de l'opération : un échange, qualification juridique qui permet – avec la « *distancia loci* » - d'éviter les foudres du droit canonique prohibant le prêt à intérêt.

[133] L'intérêt du signataire a l'opération commerciale n'a pas a être recherché : Com. 1er, Oct. 1996, Bull. n° 219 ; *RTD com*. 1997. 120, obs. Cabrillac ; *D. aff*. 1996. 1291. Mais le signataire n'acquiert pas pour autant la qualité de commerçant : v. Com. 11 mai 1993, *Bull*. n° 179 ; *RTD com*. 1994. 75, obs. Cabrillac et Teyssisé.

[134] Code de l'Organisation Judiciaire, [En ligne : http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071164&dateTexte=20080505].

- Rapport cambiaire entre le tiré et les endossataires ;

247. Dans cette opération tripartite, la lettre de change est créée d'abord en raison de l'existence d'un rapport fondamental ; il s'agit du rapport préexistant entre le tireur et le tiré, ou pour être plus précis de la dette du second envers le premier. Ce rapport fondamental est parfois reconnu par le tiré au moyen d'une acceptation. L'acceptation se définit ici comme un engagement souscrit par le tiré de payer le montant de la lettre de change à l'échéance. Elle fait naitre contre le tiré un engagement cambiaire, indépendant de toute idée de provision[135]. Le porteur aura ainsi face à lui un nouveau débiteur principal ; sa garantie de paiement sera augmentée.

248. Le plus souvent, le tireur est un vendeur de marchandises et le tiré n'est que l'acheteur. Le titre permet au vendeur qui a fait crédit à son acheteur de mobiliser sa créance. Lors de l'émission d'une lettre de change, une provision sera déposée chez le tiré, ou au plus tard elle le sera au jour de l'échéance de la traite. De son côté, le tireur remet la lettre de change à un bénéficiaire, car celui-ci lui fournit ou lui fournira une contrepartie. En cas d'endossement, l'endosseur transmet l'effet à un nouveau porteur, car il est, ou il sera, tenu à son égard.

249. En droit français, le législateur n'a pas accordé une définition légale à la lettre de change. Il a pour autant précisé le contenu de l'instrument pour lui attribuer le titre de lettre de change. C'est dans le texte de l'*article L 511-1 du Code de commerce*[136] que les critères de la lettre de change sont expressément énumérés. Ainsi afin de reconnaitre une lettre de change, il faut satisfaire les critères de validité attribués par la loi.

[135] Com. 13 mai 1996, *Bull. Civ*. IV, n°88.
[136] Article L. 511-1 du Code de commerce, version consolidée au 20 octobre 2016, *Edition Dalloz*, [En ligne:http://legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000005634379&idArticle=LEGIARTI000006233040&dateTexte=&categorieLien=cid].

B. Les exigences de forme d'une lettre de change

250. La lettre de change est un titre qui, comme tout acte juridique, doit répondre à certaines conditions de forme pour lui attribuer une valeur juridique, lui garantissant son applicabilité et sa force contraignante.

251. En droit français, l'*article L. 511-1 du Code de commerce*[137] prévoit une liste très exhaustive de mentions obligatoires devant figurer sur une lettre de change ; lorsqu'une des mentions obligatoires fait défaut, le titre ne vaut pas comme lettre de change, ce qui conduit à envisager les sanctions encourues en cas de non-respect de ce formalisme, et ainsi de déterminer l'étendue des sanctions qui peuvent être prononcées en la matière.

252. Au fur et à mesure de la présentation de critères de forme de la lettre de change, on visite la lettre de change sous sa forme électronique pour clarifier leurs conditions de validité par rapport à l'écrit sous forme manuscrit. C'est qu'un 'document transférable électronique' doit répondre aux mêmes conditions particulières de lisibilité et de présentation que celles imposées au document papier. En application du principe du parallélisme de forme, un DTE doit satisfaire les caractères essentiels d'une lettre de change pour reconnaitre sa forme électronique.

253. Il convient ici de souligner que la lettre de change fait aussi l'objet d'une loi uniforme la régissant avec les billets à ordre, transcrivant les mêmes exigences de forme indiquées à l'*article L. 511-1 du Code de commerce* (*article 1er de la Convention de Genève portant loi uniforme concernant la lettre de change et le billet à ordre*). Tous les éléments indiqués dessous doivent figurer dans les 'documents transférables électroniques'. Nous examinerons ces exigences dans l'ordre suivant :

[137] Article L. 511-1 du Code de commerce, version consolidée au 20 octobre 2016, *Edition Dalloz*.

- *Dénomination de « lettre de change »* :

254. Etant une exigence qui découle du droit uniforme issu des Conventions de Genève, la dénomination de la lettre de change[138] doit être insérée clairement dans le texte même de la lettre, et qu'un simple intitulé hors texte ne suffirait pas en soit pour caractériser une lettre de change.

255. De plus, le premier alinéa de l'article L511-1 exige que la dénomination « lettre de change » soit exprimée dans la même langue employée pour la rédaction de la lettre. L'intérêt de cette exigence est de ne pas employer une langue inconnue dans le titre, que tout soit clair pour les parties contractantes. Il y a aussi le soin de protéger le rédacteur (le tireur) et les différents signataires (les tiers bénéficiaires et éventuels endossataires) du titre contre tout vice qui pourrait en résulter ; les parties prennent conscience de la nature juridique et la rigueur des engagements qu'elles contractent ; qu'il s'agit bien d'une lettre de change qui produira des effets spéciaux répondant à des exigences particulières issues de droit cambiaire.

256. Si nous parlons d'une lettre de change électronique, le titre doit aussi contenir clairement la dénomination « lettre de change » dans le texte même du titre et que cette dénomination soit exprimée dans la même langue employée pour la rédaction du titre.

257. Afin de faciliter la circulation internationale des lettres de change, des règles d'encaissement du papier commercial unifiées ont été proposées par les banques et établissements financiers et qui avaient abouti dans une recommandation du Conseil de la Chambre de Commerce Internationale.[139] De même, pour les lettres de change par voie électronique, la loi uniforme issue de la convention de Genève avait pour objectif de faciliter leur circulation au-delà du cadre national.

[138] Une décision isolée a jugé que la mention «traite » était équivalente (Montpellier, 24 nov. 1953, *Banque* 1956. 520), solution qui doit être désapprouvée tant elle ruine la sécurité inhérente au formalisme.
[139] V. J.-Cl. *Banque*, fasc. 12.

258. Le Professeure Stoufflet a aussi précisé dans son ouvrage sur les instruments de paiement et de crédit[140] que l'exigence de l'article L 511-1 1º concernant la dénomination de la lettre de change sert essentiellement à faciliter la circulation de l'effet – et ceux qui le souscrivent qui pourraient facilement être avertis de la nature de leur engagement, un formalisme strict, mais qui répond suffisamment aux fonctions de la lettre de change.

- *Mandat pur et simple de payer une somme déterminée*

259. L'*article L.511-1 2º du Code de commerce* prévoit que la lettre de change comporte un mandat, voire un ordre adressé au tiré de payer une telle somme. Cette somme doit être déterminée en chiffre ou en lettre ; et lorsque les deux mentions figurent dans le titre de façon contradictoire, la mention en lettre prévaut[141] (*Art. L511-4 alinéa 1er C.com*).

260. D'ailleurs, si le montant est mentionné plusieurs fois, ou que nous sommes dans un cas de discordance entre les deux mentions en lettre et en chiffre, c'est le montant le plus faible qui sera retenu[142].

261. Les juristes ont l'habitude d'exiger que le montant de la lettre de change figure à la fois en lettre et en chiffres dans leurs engagements contractuels. Pourtant cette pratique devient moins courante car nous avons remarqué qu'il y a des grandes entreprises qui ont abandonné cette pratique et qui acceptent aujourd'hui de mentionner uniquement le montant de l'engagement en chiffre dans leurs engagements contractuels[143].

262. Un mandat pur et simple signifie qu'une lettre de change qui ne comporte pas un ordre explicite de payer ne pourrait valoir comme lettre de change. Cela veut dire qu'une lettre de change ne peut pas être assujettie à des conditions

[140] Gavalda et Stoufflet, *Instruments de paiement et de crédit : Litec, 8e éd. 2012*, p. 29.
[141] Com. 13 janv. 1982, JCP 1982. IV. 114.
[142] Article L 511-4 du Code de commerce.
[143] La société informatique américaine '*Oracle Systems Limited*' a abandonné depuis l'année 2015 la mention obligatoire du montant du contrat en chiffre et en lettre, en admettant de mentionner le montant uniquement en chiffre dans les contrats avec leurs clients et fournisseurs.

suspensives[144] ; et que si des conditions sont stipulées dans le titre même, ce dernier ne vaudra pas comme lettre de change.

263. De plus, le mandat de payer doit porter sur une somme déterminée ; qu'il ne suffit pas que la lettre de change comporte uniquement les éléments permettant le calcul de son montant au moment du paiement.

264. Dans ce sens, l'*article L.511-3* du Code de commerce prévoit que toute stipulation de produire des intérêts dans une lettre de change est réputée non écrite ; cette interdiction est justifiée par le fait que les intérêts rendent indéterminé le montant de la lettre de change et prive ainsi le titre, lors de son émission de la fixité de son montant. Le même article admet seulement l'introduction des intérêts dans le titre à condition que le taux des intérêts soit indiqué dans la lettre. (*Art. L.511-3 al. 2 C.com*) ce qui rend le calcul du montant exact du titre déterminable.

265. Par ailleurs, lorsque nous nous interrogeons sur les règles concernant les montants exprimés en monnaie étrangère. En ce cas, la conversion en euros s'effectuera au jour de l'échéance, sauf en cas de liquidation judiciaire ; le législateur français a transcrit cette règle dans l'*article L. 622-22, alinéa 2 du Code de commerce* en imposant la conversion au jour du jugement la prononçant.

- *Nom de celui qui doit payer la lettre de change (le tiré)*:

266. Dans une lettre de change, il faut designer celui qui doit normalement payer le titre à l'échéance ; l'identification du tiré est donc une mention indispensable pour valider le titre[145].

267. Cette exigence est interprétée de manière très stricte par la jurisprudence[146]. L'indication du domicile du tiré ne pourrait pas suppléer l'absence d'indication

[144] La notion de condition suspensive est définie dans le code civil français, dans son article 1181 qui prévoit que '*l'obligation contractée sous une condition suspensive est celle qui dépend ou d'un événement futur et incertain, ou d'un événement actuellement arrivé, mais encore inconnu des parties*'.
[145] ROBLOT (R.), «*Fasc. 425 : LETTRE DE CHANGE – Acceptation », JCP,* 2 Juin 2014, *LexisNexis SA*. n°71.

de son nom, mais qui servira comme complément d'identification. De même avec la signature du tiré sur le titre qui ne pourrait pas, à elle seule, suppléer l'absence de sa désignation, en raison d'importants risques de fraude[147].

268. De même pour la lettre de change sous forme électronique, l'identité du tiré doit figurer sur le titre de manière claire et non équivoque.

269. - *La mention de l'acceptation* - Il ne suffit pas que le nom de tiré soit mentionné sur le titre pour admettre un engagement cambiaire. Il est aussi impératif que *l'acceptation est exprimée sur le titre lui-même par le mot « accepté » ou toute autre mot ou formule équivalent impliquant l'engagement de payer du tiré*[148]. L'acceptation doit être écrite et non verbale, sinon le titre ne constituerait pas un engagement cambiaire mais de droit commun[149].

270. - *L'indication de l'échéance* - Il s'agit ici de l'indication de l'époque à laquelle le paiement peut être réclamé au tiré[150]. Cette exigence de faire figurer la date d'échéance sur la lettre de change est justifiée par deux raisons principales :

271. D'une part, l'indication de la date d'échéance tient au rôle principal attribué à la lettre de change en tant qu'un instrument de crédit à court terme, et que sa période de validité doit être limitée dans le temps.

272. D'autre part, cette indication répond aussi à la nature bien stricte et rigoureuse de la lettre de change ; c'est qu'il s'agit d'un engagement cambiaire interdisant tout délai de grâce, et supposant que la date d'exigibilité de la créance soit fixée dès l'émission du titre. Bien que les textes de la loi ne fixent aucune limite, l'échéance ne pourrait pas dépasser plus de quelques mois de la création de la lettre.

---

[146] Amiens, 15 oct. 1993 : *JCP* 1994. II. 22258, note Mossot-Durin.
[147] Comp. Com. 18 janv. 1994, *RJDA* 1994. 540.
[148] ROBLOT (R), *«Fasc. 425 : Lettre de Change – Acceptation », JCP, 2 Juin 2014, LexisNexis SA*, n° 70.
[149] *T. com. Lyon, 9 févr. 1970 : Banque 1970, p. 816,* obs. X. Marin *; RTD com. 1970, p. 750, n° 1,* obs. M. Cabrillac et J.-L. Rives-Lange.
[150] BONHOMME (R.), *Instrument de crédit et de Paiement*, 10e éd. *L.G.D.J* – 2013 – p. 102.

273. D'ailleurs, la stipulation de l'échéance dans l'*article L.511-1 du Code de commerce* a une portée large et générale, complétée par une série de textes qui prévoient quatre façons d'indiquer l'échéance et ainsi de tirer une lettre de change (*article L. 511-22 e s.*) : à vue, à un certain délai de vue, à un certain délai de date, ou à jour fixe. L'échéance doit être unique, à peine de nullité (*article L. 511-22-II du Code de commerce*[151]).

- *Indication à vue (art. L. 511-23 C.com)* La lettre est payable dès qu'elle est présentée au tiré par le porteur, et elle peut l'être à tout moment car le bénéficiaire ou le porteur choisit librement la date à laquelle sera présentée au paiement la lettre de change, dans l'année de création, sauf mention contraire apposée sur le titre.
- à jour fixe : c'est la façon la plus simple qui est l'indication du jour de l'échéance sur le titre.
- à un certain délai de date: dans cette hypothèse, le délai indiqué sur le titre court à compter de la date de création de la lettre obligatoirement mentionnée (ex. à 45 jours ou à un mois à compter de 1er janvier 2018)
- à un certain délai à vue : l'art. *L.511-24 du Code de commerce* dispose que l'échéance d'une lettre de change à un certain délai de vue est déterminée, soit par la date de l'acceptation, soit par celle du protêt[152] ; cela signifie que la lettre est payable tant de jours ou de mois à compter de son acceptation par le tiré ou de la constatation de son refus de l'accepter.

  Pareillement, une lettre de change électronique doit prévoir une date d'échéance en recourant à l'une des trois formes ainsi présentées ci-dessus.

274. - *Indication du lieu de paiement* - il s'agit d'une exigence traditionnelle maintenue par la Conventions de Genève dont l'intérêt est uniquement de renseigner le porteur sur le lieu où doit s'effectuer le paiement.

[151] Article L. 511-22 du Code de commerce, version consolidée au 20 octobre 2016.
[152] Le protêt est acte authentique dressé par un huissier à la demande du porteur d'un effet de commerce, d'une lettre de change ou d'un chèque pour constater, après sommation, soit le non-paiement à l'échéance de l'effet (protêt faute de paiement), soit le refus d'acceptation d'une traite. Voir la définition sur le site www.cnrt.fr.

275. En principe, une lettre de change doit comporter cette indication à peine de nullité ; pourtant cette nullité est rarement prononcée dans la mesure où l'*article L.511-1 alinéa 4 du Code de commerce*[153] dispose qu'à défaut d'indication du lieu du paiement, le lieu désigné à côté du nom du tiré est réputé être le lieu du paiement en même temps que le domicile du tiré. Cette présomption du lieu de paiement est maintenue lorsque nous envisageons le cas d'une lettre de change électronique.

276. - *Nom du bénéficiaire* - Au sens de l'*article L.511-1 alinéa 1er, 6o du Code de commerce* la lettre doit indiquer le « *nom de celui auquel ou à l'ordre duquel le paiement doit être fait* ». le droit français a exigé, à peine de nullité[154], la désignation du bénéficiaire, conformément aux exigences du droit uniforme, en interdisant la création de lettre de change « en blanc », à la différence du droit anglo-saxon qui admet une telle technique.

277. D'ailleurs, la jurisprudence se satisfait parfois de désignations approximatives, en acceptant que le premier endosseur remplisse l'office du bénéficiaire manquant[155]. Ici la différence entre les deux systèmes parait faible, puisque déjà la clause à ordre est incluse dans la lettre de change, le nom du porteur ne sera indiqué que lors d'un endossement. Dans ces conditions, la pratique incontestée des endossements en blanc revient à transformer, après son émission à bénéficiaire dénommé, une lettre de change en titre au porteur.

278. De plus, le bénéficiaire peut valablement être le tireur lui-même (*art. L.511-2 alinéa 1 du Code de commerce*), ainsi la pratique des endossements en blanc d'une lettre de change désignant le tireur comme bénéficiaire revient à créer une lettre de change au porteur.

---

[153] V. aussi Article 2 de la Convention de Genève portant loi uniforme sur les lettres de change et billets à ordre, *Genève*, 7 juin 1930 : https://treaties.un.org/Pages/LONViewDetails.aspx?src=LON&id=547&lang=fr.

[154] Est nul le titre qui ne contient pas le nom de celui auquel ou à l'origine duquel, le paiement doit être fait : Com. 6 juil. 1965, *D.* 1966. 24.

[155] Désignation par la signature d'endossement du tireur, Com. 9 mars 1976, *Bull.* no85 ; *RTD com.* 1976. 754, obs. Cabrillac et Rives-Lange ou par celle du souscripteur du billet à ordre, l'identité entre souscripteur et bénéficiaire n'étant pas prohibée et l'endossement du souscripteur le désignant lui-même implicitement comme bénéficiaire : Com. 13 sept, 2011, no10-19963, *Bull.* no129 ; *D.* 2011, act. 2269, obs. Delpech ; *JCP G* 2011. 1046, obs. Lasserre Capedeville ; *Banque et Dr*. Nov. 2011, 15 obs. Bonneau ; *Gaz. Pal.*, 28 oct. 2011. 31, n. Houin-Bressand.

279. - *Le lieu et la date de création de la lettre de change* - Si nous supposons que l'indication du lieu de création de la lettre de change est presque sans intérêt dans les relations internes, elle est par contre très utile et son importance surgit lorsque nous sommes en mesure de régler un conflit de lois dans une relation internationale. Comme par exemple lorsque la lettre est payable dans un pays autre que celui de sa création. Dans ce cas, ça sera le lieu d'émission de la lettre de change qui détermine la loi applicable aux rapports cambiaires.

280. D'après l'article L. 511-1 alinéa 5 du Code de commerce, lorsque le lieu de création n'est pas indiqué sur la lettre de change, celle-ci doit être considérée comme souscrite dans le lieu désigné à côté du nom du tireur.

281. Evidemment, la mention du lieu de la création du titre est assez importante si nous envisageons le cas d'une lettre de change électronique ; cette importance est due à la nature du titre électronique lui permettant d'entrer dans des relations transnationales dépassent facilement les frontières étatiques d'un pays.

282. Concernant la date de création de la lettre, il est très important de dater une lettre de change, et cela s'explique pour plusieurs raisons. D'abord la mention de la date de création est importante pour apprécier la capacité des parties au moment de la création de la lettre, permettant de vérifier si le tireur avait, au moment de la création de la lettre de change, la capacité et le pouvoir de l'émettre.

283. La date de création sert aussi à déterminer l'échéance de la lettre. Elle permet de prévoir le délai de présentation au paiement pour les lettres de change créées à vue ; à cet égard, la date de création mentionnée dans la lettre constitue le point de départ du délai d'un an.

284. En cas d'omission de date, une jurisprudence constante décide que la lettre de change est nulle[156] et que le titre ne peut plus valoir comme lettre de change. Il est ainsi indispensable de mentionner la date de création du titre dans une

[156] Com. 9 mai 1962, *Bull. civ. III*, n° 247. Com. 7 nov. 1979, *Gaz. Pal.* 1980. 1.44, note J.D. ; *RTD com*. 1980. 115, obs. Cabrillac et Rives-Lange. Com. 29 juin 1983, Bull. civ. IV, n° 198. Com. 13 mars 1985, *Bull. civ. IV*, n°97; *D.* 1985. IR. 418, obs. Cabrillac. Com. 7 oct. 1987, *D.* 1988. Somm. 51, obs. Cabrillac.

lettre de change électronique pour les mêmes raisons que nous venons d'évoquer pour la lettre de change manuscrite.

285. - *Signature du tireur* - Le tireur doit apposer sa signature sur le titre. Cette exigence de la signature du tireur est primordiale pour matérialiser l'engagement cambiaire du tireur puisqu'il est le premier à s'obliger cambiairement.

286. A ce propos, le législateur français a reconnu implicitement l'utilisation de la signature électronique lorsqu'il prévoit dans le même article que la signature peut être apposée, soit à la main, soit après tout procédé non manuscrit.

287. Il faut ici préciser que l'indication du nom et du domicile du tireur ne suffirait pas pour suppléer l'absence de signature. Si la signature est absente, la lettre de change ne vaut pas comme titre cambiaire ; le titre vaudra cependant comme une simple reconnaissance de dette.

288. En apposant leur signature, les parties expriment leur accord sur la nature cambiaire de leur engagement. Or, la signature par chacune des parties est irremplaçable tant pour une lettre de change papier ou par voie électronique afin de produire ses effets juridiques.

289. Le respect de tous ces critères susmentionnés qui relèvent de la forme de la lettre de change est impératif pour reconnaitre le titre et la nature particulière de l'engagement cambiaire ; la lettre de change par voie électronique n'en fait pas exception, qu'elle devrait obéir à l'ensemble de ces règles régissant son équivalent sous forme manuscrite.

C. Les exigences de fond d'une lettre de change

290. Comme tous les actes juridiques, la lettre de change doit répondre aux conditions générales de validité des actes juridiques touchant la capacité, les pouvoirs, le consentement, l'objet et la cause.

1) Le consentement du tireur

291. Le consensualisme est un principe fondamental en droit civil, selon lequel un contrat se forme par le seul échange de consentement sans qu'aucune forme particulière ne soit nécessaire ; et qu'en vertu de ce principe, un document écrit et signé n'est pas une condition de formation du contrat. Que tout contrat est consensuel à moins que la loi dispose autrement.

292. La lettre de change repose sur le consentement du signataire[157]. Le consentement doit répondre aux conditions de droit commun des obligations : c.-à-d. que l'expression du consentement est réelle et exempte de vices au sens de l'*article 1109 du Code civil*[158].

293. L'absence de consentement est sanctionnée en droit commun par la nullité absolue[159]. Nous entendons par nullité absolue que toute personne intéressée peut invoquer cette nullité ; aussi le juge peut la prononcer d'office, et que le délai de prescription est de cinq (5) ans d'après l'*article 2224 du code Civil*.

294. En principe, un titre nécessite un consentement non vicié de la part de son auteur (le tiré dans une lettre de change). Que ce consentement se matérialise essentiellement par sa signature qui est un des critères de forme, prévu à l'*article L. 511-1-8º du Code de commerce*. Un acte juridique ne peut pas produire pleinement ses effets s'il y a un vice de consentement.

---

[157] Gavalda et Stoufflet, *Op. Cit.*, p.55.

[158] Code civil, version consolidée au 9 octobre 2016.. [En ligne : http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070721].

[159] J. Flour et J.-L. Aubert, *les obligations, l'acte juridique*, 8e éd., *Armand Colin*, 1998, nº344 ; selon la doctrine, la nullité relative correspondait davantage à la sanction d'un défaut portant atteinte ici à un intérêt particulier.

295. D'ailleurs, une lettre de change est un acte de nature cambiaire, ce qui lui fait exception à la règle ; bien qu'un vice de consentement soit caractérisé dans le rapport fondamental entre le tireur et le tiré, la lettre de change est en mesure de produire pleinement ses effets cambiaires à l'égard des autres parties signataires. Cela s'explique par deux notions qui caractérisent l'engagement cambiaire :

296. D'une part, il s'agit du principe de l'***indépendance des signatures***. Aux termes de l'article L 511-5 du Code de commerce : « *Quiconque appose sa signature sur une lettre de change comme représentant d'une personne pour laquelle il n'avait pas le pouvoir d'agir, est obligé lui-même en vertu de la lettre et, s'il a payé, a les mêmes droits qu'aurait eus le prétendu représenté. Il en est de même du représentant qui a dépassé ses pouvoirs* ».

297. Ce principe, comme définit par l'article susmentionné, signifie que la validité de l'engagement de chaque signataire est traitée séparément ; que chacune des parties est engagée par ce qu'elle a signé indépendamment des autres parties, même si les autres engagements sont atteints d'une cause de nullité, et quelle que soit la cause de la nullité invoquée (que ce soit l'incapacité, consentement vicié ou la fausse signature, etc.). Cette règle renforce considérablement le titre et constitue l'un des piliers de la sécurité juridique que la loi a accordée au porteur dans un engagement de nature cambiaire[160].

298. D'autre part, la règle de l'***inopposabilité des exceptions*** est une autre notion qui caractérise l'engagement cambiaire. D'après ce principe, Les personnes actionnées en vertu de la lettre de change (ex : tiré accepteur, endosseur, tireur), ne peuvent pas opposer au porteur les exceptions fondées sur leurs rapports personnels avec le tireur ou avec les porteurs antérieurs. En effet, il y a purge des exceptions à chaque transmission. Ainsi ce principe de l'inopposabilité des exceptions ne donne pas le droit aux parties de se prévaloir

[160] Par ex., en cas d'émission au nom d'une société par une personne sans pouvoir, l'obligation au paiement du tiré accepteur reste valable : Com. 15 juin 1993, *Bull.* n° 247 ; *RTD com.* 1993. 690, obs. Cabrillac et Teyssié.

d'un vice quelconque sur un rapport antérieur pour contester l'acte vis-à-vis d'un porteur de bonne foi.

299. Cette solution est retenue par la convention de Genève en 1930 portant loi uniforme sur les lettres de change et billets à ordre, dans son article 10[161] qui prévoit que « *Si une lettre de change, incomplète à l'émission, a été complétée contrairement aux accords intervenus, l'inobservation de ces accords ne peut pas être opposée au porteur, à moins qu'il n'ait acquis la lettre de change de mauvaise foi ou que, en l'acquérant, il n'ait commis une faute lourde* ». Nous retenons de ce texte que lorsque le porteur est de bonne foi et n'a pas commis une faute qualifiée de grave, il peut toujours bénéficier de principe de l'inopposabilité des exceptions pour demander l'exécution de la lettre.

300. L'absence de consentement dans un acte juridique peut prendre plusieurs formes :

1) Falsification de signature

301. La règle de droit dicte ici que nous ne pouvons pas imposer au tireur d'honorer un engagement qu'il n'a pas consenti ou dont le consentement est vicié.

302. Dans la doctrine si une falsification de la signature est caractérisée dans une lettre de change, le tireur ne pourra pas être engagé cambiairement, lorsqu'il n'a pas donné son consentement à la création du titre[162]. Par contre sa responsabilité civile pourra être engagée s'il a, par ses agissements, facilité la falsification de l'acte. Or l'acte falsifié reste valable vis-à-vis des autres signataires par application du principe de l'indépendance des signatures.

303. - *Signature contrefaite* - La contrefaçon de la signature est un autre exemple de consentement vicié. Dans cette hypothèse, la sécurité du porteur de bonne foi cède devant celle de la personne dont la signature a été imitée, qui ne

[161] Convention portant loi uniforme sur les lettres de change et billets à ordre (Genève, 7 juin 1930), [En ligne: http://www.admin.ch/opc/fr/classified-compilation/19300022/200508170000/0.221.554.1.pdf]
[162] Putman, n°53; Gavalda et Stoufflet, *Op. Cit.*, n°32 et en jurisprudence Civ. 17 déc. 1884, *DP* 1885. 1. 102.

sera pas engagée et peut opposer au porteur cette nullité, peu importe que l'imitation ait été parfaite.

304. Cependant le porteur peut, en certains cas, rechercher la responsabilité civile du tireur prétendu (ex. : comme dans le cas de falsification de signature, si le tireur du titre a, par sa négligence, facilité les agissements du faussaire ; ou au titre de la responsabilité des commettants) ; la responsabilité pénale du faussaire pourra aussi être engagée, comme celle des personnes qui feraient sciemment usage du titre falsifié[163]

305. - *Altération de la lettre de change* - La même solution similaire est retenue en cas d'altération de la lettre de change. L'altération se définit comme une modification du texte initial de la lettre de change sans le consentement du tireur ou des signataires antérieurs*[164]*.

306. D'après l'article *L. 511-77* du Code de commerce, les signataires postérieurs à l'altération seront tenus dans les termes du texte altéré et que les signataires antérieurs, donc le tireur, le sont dans les termes du texte originaire, c.-à-d. à hauteur de ce qui ressort du titre au moment où ils le signent, même si le porteur est de bonne foi[165].

307. Une altération de l'effet implique une modification importante dans le sens où elle aura pour effet de modifier la situation juridique d'un ou plusieurs signataires de la lettre de change. Les altérations les plus fréquentes se produisent sur le montant de la lettre et sur la date d'échéance. Si par exemple l'une des parties ajoute un zéro à la somme figurant sur le titre, ça doit caractériser une altération significative à l'acte ; alors dans ce cas l'engagement du tireur se limite au montant figuré dans le texte primitif, et il ne peut pas être

[163] Faux en écriture de commerce; Code pénal, art. 441-1 et s. ; v. sur ces aspects, M. Cabrillac et C. Mouly, Droit pénal de la Banque et du Credit, Masson, 1982, n°349 ; v. une application par Com. 2 déc. 1997, *JCP E* 1998. 151, où il est jugé que les juridictions civiles doivent surseoir a statuer jusqu'à l'issue de la procédure.
[164] Le Cannu (P.), Granier (T.), Routier (R.), *Op. Cit.*, p. 301.
[165] Com. 11 janv. 1972, *Bull.civ. IV*, n°17; Com. 12 oct. 1993, *JCP* 1995. II.22378, note Bazin ; Régine Bonhomme, *Instrument de crédit et de Paiement*, 10e éd. *L.G.D.J* – 2013, p. 111.

engagé à honorer la lettre dans sa nouvelle forme modifiée à son insu, même à l'égard d'un porteur de bonne foi.

2) La capacité des parties

308. La question de capacité se pose principalement pour protéger les intérêts des personnes vulnérables lorsqu'elles s'engagent à travers des actes juridiques. Et pour reconnaitre la validité d'une lettre de change, il faut rechercher la capacité requise pour contracter un engagement cambiaire.

- Le mineur

309. Comme la lettre de change s'analyse en un acte de commerce par la forme, le tireur doit avoir la capacité pour effectuer des actes de commerce[166] ; il n'est pas nécessaire pour autant qu'il ait la qualité de commerçant.

310. D'après le premier alinéa de l'article L. 511-5[167] du Code de commerce, les lettres de change souscrites par des mineurs sont nulles à leur égard, sauf les droits respectifs des parties.

311. Il s'agit là pour la plupart des auteurs d'un texte de portée générale dans le sens où un mineur ne peut souscrire une lettre de change, même à titre occasionnel, car d'après l'article L. 110-1 du Code de commerce, cette incapacité générale d'exercice du mineur repose sur le fait que la signature d'une lettre de change est un acte de commerce par la forme. Un tel acte ne pouvait être accompli ni par le mineur émancipé (sauf s'il était commerçant avec une autorisation spéciale), ni même par son représentant légal.[168]

312. La nullité de l'engagement cambiaire du mineur est ici une nullité de protection, donc d'une nullité relative, conformément au droit commun des

[166] Sur l'aptitude du mineur à passer des actes de commerce, Piedelièvre, *Actes de commerce, commerçants et fonds de commerce,* 7e éd., no58 ; sur la solution en matière de lettre de change, Roblot, no97 ; Jantin et le Cannu, no289.

[167] L'article L. 511-5 alinéa 1er du Code de commerce dispose que « *Les lettres de change souscrites par des mineurs sont nulles à leur égard, sauf les droits respectifs des parties, conformément à l'article 1312 du code civil* ».

[168] Ribert et Roblot, *Traité de droit commercial,* t. I, vol.1 par L. Vogel, 19e éd., no 389. Y. Chaput, *Effets de commerce, Chèques et Instruments de paiement et de crédit, Titrisation, Dalloz,* 8e éd., no 353.

obligations. Seul le mineur ou son représentant légal peut invoquer la nullité du titre dans un délai de cinq (5) ans à partir du jour de la conclusion de la lettre.

313. Donc nous retenons le principe selon lequel un mineur émancipé ne peut pas valablement signer une lettre de change pour un acte qu'il n'a pas la capacité d'accomplir seul, et son représentant légal ne pouvait pas l'engager dans une opération cambiaire [169].

314. Pourtant, le législateur français, dans une hypothèse bien particulière[170], s'est montré en faveur de la validité de la signature du mineur à condition que celui-ci soit autorisé à exercer le commerce par ses représentants légaux ou exerce le commerce avec l'assentiment du juge de tutelle ou du président du tribunal de grande instance, ainsi que le permettant dorénavant les articles modifiés *413-8 du Code civil* et *L. 121-2 du Code de commerce* (v. aussi, *C. civ., art. 389-8, 401 et 408*).

315. D'ailleurs, la nullité de l'engagement de l'incapable est opposable au porteur de bonne foi[171] ; la protection de l'incapable doit prévaloir sur celle du porteur. Ce dernier a pourtant d'autres voies de recours à l'encontre des autres signataires[172] (*art. L.511-5 al. 2 C.com* : principe d'indépendance des signatures) et, le cas échéant, il bénéficie aussi des actions extra-cambiaires réservées par les articles *1310 et 1312* du Code civil.

316. De plus, il est encore possible d'invoquer à l'encontre du mineur les règles de l'action de *in rem verso (enrichissement sans cause)*, s'il a tiré un enrichissement du fait de sa signature sur l'effet. En tout état de cause, si le mineur commet un délit ou un quasi-délit lors de sa signature sur l'effet, il doit réparer le préjudice qu'il a causé au porteur.

---

[169] Pour l'affirmative, v. J. Stoufflet, n° 28, qui se fonde notamment sur l'abrogation par la loi du 5 juil. 1974 de l'article 3 du Code de commerce. Contr, P. Delebecque et M. Germain, n° 1959, pour qui « *le désir d'épargner aux incapables les rigueurs spéciales du droit de change* » interdit au représentant d'engager l'incapable ; M. Cabrillac, *La lettre de change dans la jurisprudence*, n°1, p. 13 s.

[170] Loi n°2010-658 du 15 juin 2010 relative à l'entrepreneur individuel à responsabilité limitée.

[171] L'incapable peut opposer son incapacité à tous, même au tiers porteur de bonne foi. Civ. 19 févr. 1869 : *DP* 1856.1.86. Paris, 17 juill. 1894 : *DP* 1895.2.25, note Thaller Paris, 10 nov. 1925 :*DP* 1926.2.139, note H.L.

[172] Com. 21 dec. 1959, *D.* 1960.262.

317. Pour admettre une action *in rem verso* à l'encontre de mineur, le juge français exige la preuve que ce mineur avait conscience de sa faute[173]. Cette solution retenue vaut non seulement pour les incapables mineurs, mais aussi pour les incapables majeurs (*art. L. 511-5 al. 2 C.com*) auxquels le législateur a assimilé les consommateurs qui ont recours à certains crédits (immobiliers ou à la consommation).

- Majeurs incapables

318. Concernant les personnes majeures protégées, il est nécessaire de distinguer suivant le régime de protection. L'engagement du tireur de la lettre de change peut-être annuler sur le fondement de l'*article 414-1 du Code civil*, si la preuve a été apportée que son consentement a été donné à un moment où il souffrait d'un trouble mental.

319. L'*article 473 du Code civil* frappe le majeur en tutelle d'une incapacité générale. Il lui est ainsi impossible d'émettre une lettre de change.

- Le Consommateur

320. Pour le consommateur, l'*article L.313-13 du Code de la consommation* fait référence à l'*article L.511-5 du Code de commerce* pour accorder le même traitement de mineurs aux consommateurs pour les lettres de change et les billets à ordre souscrits par les emprunteurs même majeurs à l'occasion des opérations de crédit à la consommation ou de crédit immobilier.

321. Ainsi dans ces hypothèses susmentionnées le législateur a assimilé le consommateur à un mineur, voire à une personne incapable. La Cour de cassation a précisé que cette interdiction s'applique aussi bien pour les effets souscrits (ou avalisés) lors de l'octroi du crédit que pour ceux qui le seraient postérieurement[174].

[173] Req.15 nov. 1898 et 21 mars 1899, S. 1899. 1. 225, note Wahl.
[174] Civ 1ère, 30 sept. 1997, *RTD com.* 1998.181, obs. Cabrillac.

322. A l'inverse, une directive européenne du 22 décembre 1986 sur la protection des consommateurs[175] permet l'utilisation des lettres de change, même si elle autorise les Etats membres à prendre des mesures plus strictes, dans un but de protection, que celles contenues dans la directive.

3) Les pouvoirs

323. Le pouvoir se présente en général comme une prérogative permettant à une personne d'effectuer des actes juridiques pour le compte d'autrui[176]. Il est très fréquent qu'un tireur souscrive une lettre de change pour le compte d'autrui. C'est bien souvent le cas lorsque la lettre est émise par le représentant légal d'une personne morale.

324. Nous examinons ici deux hypothèses dans lesquelles le tireur se trouve représenter par un mandataire qui agit vis-à-vis des tiers :

325. - *Tirage de la lettre de change par un mandataire* - Le tirage par l'intermédiaire d'un mandataire se caractérise généralement par la signature du mandataire précédé de la formule « par procuration » ; ainsi le tirage d'une lettre de change au nom et pour le compte d'autrui est une opération courante, que le représentant soit investi d'un mandat conventionnel, judiciaire ou légal.

326. Il s'agit d'une pratique très fréquente lorsque le tireur est une personne morale, représentée par ses dirigeants. Les limitations statutaires des pouvoirs des dirigeants de sociétés sont en principe inopposables aux tiers et un usage bancaire constant dispense le banquier escompteur[177] d'exiger la justification des pouvoirs de la personne qui a apposé la signature[178].

---

[175] Directive Européenne n°87-102 du 22 décembre 1986, *JOCE* du 12 février 1987 page 48.

[176] V. E. Garillard, *La notion de pouvoir en droit privé*, *Economica*, 1985, pref. Cornu, n°65 s. ; P. Malaurie et L. Aynes donnent une autre définition : « *aptitude d'une personne a engager des biens par ses actes (les siens ou ceux d'autrui)* », Les *obligations*, Défrenois, 4e éd., 1997, n° 803.

[177] L'escompte il s'agit d'une opération de crédit par laquelle le porteur d'une lettre de change en transfère la propriété à un banquier, qui en avance immédiatement le montant (diminué de sa rémunération) et sera remboursé à l'échéance grâce au paiement par le tiré. Définition rapportée par Régine Bonhomme, *Op. Cit.*, , n°160.

[178] V. dans ce sens, Com. 9 mars 1999, *RTD com*. 1999. 929, obs. Cabrillac ; *RDBF* 1999. 94, obs. Crédot et Gérard.

327. - *Tirage pour compte* - Le tirage pour compte est prévu à l'*article L.511-2 alinéa 3 du Code du commerce* qui dispose que la lettre de change peut-être tirée pour le compte d'un tiers ». Nous parlons de tirage pour compte lorsque le tireur qui agit pour le compte d'autrui ne révèle pas aux tiers cette qualité et se présente comme un tireur ordinaire. Cette émission se distingue de l'autre tirage par mandataire par le fait que le tireur pour compte agit personnellement comme tireur.

328. Ainsi le tirage pour compte est un cas de tirage imparfaite, occulte, qui évoque le contrat de commission dans lequel le tireur pour compte est qualifié le véritable créateur du titre, et ce n'est que lui qui apparait sur le titre. Bien que le donneur d'ordre n'apparaisse pas sur le titre, il sera tenu de fournir la provision[179].

329. Un exemple fréquent de tirage pour compte est l'hypothèse dans laquelle une convention extra-cambiaire investit un cabinet de recouvrement des créances qui se charge de recouvrer les fonds pour le compte de ses clients, donneurs d'ordre, ou bien un fournisseur qui, pour des raisons de stratégie commerciale, préfère rester caché, etc.[180]

330. Quant aux effets du tirage pour compte, en règle générale, le tireur pour compte se trouve tout seul engagé vis-à-vis des tiers et des porteurs successifs, et qu'aucune action cambiaire ne pourrait être intentée contre le donneur d'ordre puisqu'il s'agit d'un mandat occulte qui évite tout rapport juridique entre le donneur d'ordre et les tiers qui ne connaissent que le tireur pour compte.

331. Pourtant la théorie du mandat réapparait dans les rapports liant le donneur d'ordre du tiré : le tiré qui aurait payé sans avoir reçu provision a la possibilité de se retourner contre le donneur d'ordre[181]. Ainsi une restriction à la règle générale existe dans les rapports du tireur pour compte et du tiré qui doit

[179] Le Cannu (P.), Granier (T.), Routier (R.*), Op.Cit.* , p.317.
[180] V. Com. 29 nov. 1994, Bull. n° 353; *RTD com*. 1995. 173, obs. Cabrillac: tirage par le cédant Dailly pour compte du cessionnaire, après notification de la cession; le tiré accepteur peut être des lors oppose le défaut de provision au donneur d'ordre (cessionnaire de la créance) qui n'a pas la qualité d'un tiers porteur.
[181] Com. 10 mars 1970, *Bull. Civ. IV*, n°91 rejetant un pourvoi contre Paris, 24 janv. 1968, *RTD com*, 1969. 130, obs. Cabrillac et Rives-Lange.

réclamer la constitution de la provision au donneur d'ordre et non au tireur pour compte (*C. com., art. L. 511-7, al. 1^er^*). Dans ce dernier rapport entre le donneur d'ordre et le tireur pour compte, ce sont les règles extra-cambiaires du mandat qui s'appliquent puisqu'il ne s'agit pas d'un rapport cambiaire.

4) L'objet et la cause

332. Quant à l'objet de l'obligation cambiaire, elle est principalement sous forme pécuniaire caractérisé par le paiement d'une somme d'argent. L'objet doit également être licite et ne pourrait pas être le résultat d'un acte illicite ou interdit par la loi.

333. Nous citons un exemple d'illicéité de l'objet de l'obligation cambiaire lorsqu'une lettre de change est libellée en monnaie étrangère au mépris d'une prohibition de la législation des changes.

334. Concernant la cause, l'engagement cambiaire du tireur envers le bénéficiaire trouve sa cause dans un rapport juridique entre eux qui est la créance fondamentale de la valeur fournie ; ce dernier rapport doit exister et qu'il ne soit pas illicite. Que ce rapport juridique fasse défaut ou qu'il soit illicite ou immoral, l'obligation du tireur sera réputée nulle en application de l'*article 1131 du code civil*[182].

335. Cette solution est fondée sur la théorie du caractère abstrait pris par le signataire de la lettre de change le privant de la protection assurée en droit commun par la théorie de la cause.

336. Citons ici quelques exemples sur la cause illicite : le cas d'une lettre émise en vue du règlement du prix d'une maison de tolérance ou d'une clientèle médicale, dans la mesure où nous la considérons comme étant hors commerce, ou bien pour réaliser une donation prohibée ou bien encore en vue d'une dissimulation fiscale[183].

[182] Code Civil, version consolidée au 9 octobre 2016.
[183] Cass. Com., 19 juillet 1982 : Bull. civ. 1982 : *Bull. civ*. 1982, IV, n°279, p. 240.

337. Or, si l'absence ou l'illicéité de la cause est apparente sur le titre (c.-à-d. il est clairement mentionné sur le titre la consistance illicite de la valeur fournie), la nullité de l'engagement du tireur sera opposable à tous les porteurs de mauvaise foi ; les autres engagements n'étant pas affectés dans la mesure où ils n'ont pas la même cause.

338. - *Effets de complaisance* - La principale hypothèse qui soulève plus de difficultés est celle des effets dits de complaisance (c.-à-d. sans provision sérieuse), et elle concerne le plus souvent la nullité pour cause illicite ou absence de cause de l'engagement cambiaire, non du tireur, mais du tiré qui, par une complaisance coupable, s'engage à payer des effets qu'il n'a en réalité aucune intention de payer, pour l'excellente raison qu'il ne doit rien au tireur (la créance fondamental de provision n'existe pas).

339. Les effets de complaisance sont à la base un terme financier qui s'emploie dans le monde des affaires lorsque nous envisageons l'hypothèse d'un commerçant qui connait une gêne financière et qui demande à un ami de lui rendre service en l'autorisant à tirer sur lui une lettre de change bien qu'il ne soit titulaire à son égard d'aucune créance, ni présente ni en formation.

340. Cette opération s'effectue à l'insu de la banque qui ignore les conditions de l'émission en lui faisant croire que le tireur est effectivement créancier à terme d'une certaine somme sur le tiré. Ainsi le tireur, dans cette hypothèse, appelé complu, obtient grâce au tiré appelé complaisant les liquidités dont il a besoin auprès de la banque.

341. Cette opération est appelée ainsi 'effet de complaisance' à raison de sa nature frauduleuse; qu'elle consiste essentiellement à tromper les tiers, concrètement les banquiers susceptibles d'escompter ces titres, sur la réalité des relations fondamentales inexistante dans la réalité des faits. *Et comme le tiré n'a pas à payer réellement, il est convenu entre les parties qu'à l'échéance, le tireur lui fera parvenir des fonds, qu'il se procurera peut-être en tirant un nouvel effet, d'un montant un peu supérieur pour couvrir les frais ; lorsque les effets successifs se chevauchent ainsi, on parle de cavalerie. Ou bien, pour se*

rembourser, le tiré tirera sur le tireur un effet aussi fictif que le premier (tirage croisée), qu'il veillera à faire escompter par un autre banquier[184].

342. Dans cette hypothèse, en principe le tiré se trouvera valablement engagé, par sa signature, envers la banque à la hauteur du crédit qu'il a consenti au tireur; parce qu'il s'agit d'une cause licite qui découle d'un engagement indépendant du rapport principal (la créance fondamentale de provision) ; et que lorsque quoi qu'il arrive au tireur lui empêchant d'honorer sa dette envers la banque, le tiré est prêt à payer si nécessaire à la manière d'une caution.

343. Toutes ces opérations appelées des 'effets de complaisance' sont illicites[185]. L'engagement du tiré complaisant est nul de nullité absolue. Pourtant, cette nullité est inopposable au porteur de bonne foi.

344. Après avoir traité la lettre de change, nous traitons ensuite un autre titre qui fait partie de la famille 'effet de commerce', le titre 'billet à ordre' ressemble en partie à la lettre de change mais qui détient une forme assez simplifié.

[184] Régine Bonhomme, *Op. Cit.*, p. 115. Dans ce sens, voir Christine Lassalas, « Fasc. 550 : Escompte », 1er Janvier 2016, *JurisClasseur Banque - Crédit – Bourse*, n°13 : « *S'agissant d'effets de complaisance, le souscripteur n'entend pas effectuer le paiement à l'échéance. Aussi, le tireur en émettra une seconde qu'il proposera à l'escompte et fournira ainsi au tiré la somme d'argent nécessaire pour effectuer le paiement du premier effet. Cette opération, lorsqu'elle se renouvelle, aboutit à la création d'effets de cavalerie, expression justifiée par le chevauchement des effets de complaisance* ».

[185] Et peuvent être constitutive d'escroquerie si elles s'accompagnent de manœuvres frauduleuses: v. Crim. 20 juin 1983, *Bull*. no189, *RTD com.* 1984. 492, obs. Cabrillac et Teyssié ; P. Delebecque et M. Germain, no1984 et les réf. cit. ; M. Cabrillac , *La lettre de change dans la Jurisprudence*, no39, E, p. 159. Pour un exemple récent d'utilisation de lettre de change fictive : Crim. 4 avr. 2012, no11-81332, *Gaz. Pal*., 22 sept. 2012. 23 s., n. Morel-Maroger.

II. FORMATION DU BILLET À ORDRE

345. Est qualifié d'effet de commerce, le billet à ordre qui est un écrit par lequel un souscripteur s'oblige à payer une somme d'argent à l'ordre d'un preneur ou bénéficiaire, à une date déterminée et s'oblige à payer si le tiré ne le fait pas[186].

346. L'originalité du billet à ordre par rapport à la lettre de change est caractérisée par la relation bipartite réunissant uniquement un souscripteur et un bénéficiaire ; le premier s'engage cambiairement de payer à l'échéance le bénéficiaire ou toute autre personne que celui-ci se sera substitué par voie d'endossement.

347. Deux remarques peuvent ici être soulignées. D'une part, le souscripteur d'un billet à ordre cumule les qualités de tireur et de tiré ; par conséquent, la théorie de l'acceptation que nous envisageons dans le rapport tireur-tiré dans une lettre de change n'aura pas lieu dans un billet à ordre. De même avec la théorie de la provision qui n'aurait aucune signification dans un billet à ordre.

348. D'autre part, le billet à ordre établit un rapport cambiaire entre le souscripteur et le bénéficiaire, mais ce rapport n'engendre pas d'effet novateur du rapport fondamental préexistant. Alors si nous sommes dans un cas où le rapport cambiaire est anéanti, le bénéficiaire pourra toujours recourir contre le souscripteur sur le fondement du droit commun[187].

349. Le billet à ordre est un titre négociable, qui répond aux mêmes caractéristiques de la lettre de change en tant qu'effet de commerce. Pourtant, à la différence de la lettre de change, le billet à ordre présente une structure plus simple[188] car sa création n'intéresse que deux personnes dont l'une, celle qui s'engage cambiairement (le souscripteur) et qui se présente comme étant le débiteur principal de l'effet.

---

[186] Régine Bonhomme, *Op. cit.*,, n°238.
[187] Le Cannu (P.), Granier (T.), Routier (R), *Op. cit.* , n°485.
[188] J. Stoufflet, *Op. cit, n°151.*

350. Malgré quelques différences techniques, le billet à ordre et la lettre de change incorporent tous les deux une créance de somme d'argent, payable au porteur, à une date déterminée.

351. Ce rapprochement entre les deux titres se manifeste dans leur régime juridique respectif qui leur rapproche de manière significative. En fait le régime du billet à ordre est inspiré de celui de la lettre de change et suit son modèle pour produire ses effets juridiques.

352. Sont ainsi applicables au billet à ordre de nombreuses dispositions relatives à la lettre de change par renvoi exprès de textes de la loi, dès lors que ces dispositions sont compatibles avec le billet à ordre[189].

353. De ce renvoi nous saisissons deux remarques importantes : d'un côté, ce renvoi est limitatif dans la mesure où aucune autre disposition applicable à la lettre de change ne peut être transposée.

354. D'un autre côté, cette transposition ne doit pas s'effectuer de manière automatique mais plutôt raisonnée ; cela revient à dire que le renvoi est effectué aux dispositions relatives à la lettre de change dans la mesure où elles ne sont pas incompatibles avec la nature du billet à ordre[190].

Or, nous étudierons les conditions de validité d'un billet à ordre, en commençant par les exigences de forme (A) puis celles de fond (B)

A. <u>Exigence de forme du billet à ordre</u>

355. Aux termes de l'article *L. 512-8 du Code de commerce*, « *Le règlement par billet à ordre n'est permis au débiteur que s'il a été expressément prévu par les parties et mentionné sur la facture…* ». Alors d'après ce texte, un débiteur ne peut pas imposer à son créancier le paiement par billet à ordre à moins que ce

[189] *C. com., art. L. 512-3 à L. 512-8. - Conv. LU, annexe I, art. 77.*
[190] V. par ex. l'application des principes régissant la coexistence d'un effet et d'un bordereau Dailly : Com. 10 mars 1998, *RTD com.* 1998. 648, obs. Cabrillac ; *D.* 1998. 620, note Goyet.

soit expressément indiqué dans le titre et mentionné sur la facture. Il s'agit là d'une règle d'ordre public dont les parties ne peuvent pas déroger[191].

356. Toutefois, dans une décision juridictionnelle rendue par la Cour de cassation en date de 12 février 1991[192], le juge français a décidé autrement en estimant que cette interdiction n'est pas sanctionnée par la nullité du titre ; qu'il ne s'agit ni d'un vice de forme, ni d'un vice apparent pour justifier la nullité du billet en cause, et que lorsque cette interdiction n'intéresse que les rapports entre le souscripteur et le bénéficiaire, elle est donc inopposable au porteur de bonne foi.

357. De plus, l'article *L. 512-8 du Code de commerce* prévoit ensuite que lorsque les parties ont conventionnellement accepté le recours au billet à ordre, celui-ci doit être adressé par le souscripteur à son créancier dans les trente jours de l'envoi de la facture. Si ce délai impératif n'est pas respecté, le fournisseur est autorisé à émettre une lettre de change sur son client, celui-ci étant alors tenu de l'accepter.

358. L'*article L. 512-1 du Code de commerce* énumère les mentions légales obligatoires qui doivent, à peine de nullité en tant que billet à ordre, figurer sur le titre :

2) La *clause à ordre* doit figurer expressément sur le titre, mais ce peut être (*C. com., art. L. 512-1-I., 1º*) soit en tant que telle (par ex. : « Nous paierons à l'ordre de… »), soit dans la dénomination du titre (billet à ordre) insérée dans le texte (par ex. : « Contre billet à ordre, nous paierons… »).
3) *Une promesse pure et simple de payer une somme déterminée* est une mention à rapprocher du « mandat » requis dans la lettre de change ; elle doit être interprétée de la même manière (*C.com. art. L511-1-2º*). Il en est de même pour les autres mentions prévues à l'article *L. 512-1* : i.e. l'indication de l'échéance, lieu ou le paiement doit s'effectuer, nom de celui auquel ou à l'ordre duquel le paiement doit être fait, et la signature du souscripteur.

[191] Le Cannu (P.), Granier (T.), Routier (R), *Op. cit.*, nº486.
[192] Com. 12 févr. 1991, *D. 1991. Somm. 216, obs. Cabrillac; Bull.civ.IV, nº64.*

4) *Indication de l'échéance*. La détermination de l'échéance s'effectue, par renvoi de l'art. *L. 512-3*, aux *arts. L. 511-22* à *L. 511-25* concernant la lettre de change. L'échéance doit être indiquée dans le titre, sinon le billet sera réputé payable à vue (*art. L.512-1, II*).

359. Des règles particulières sont prévues par l'article L. 512-7 du Code de commerce pour la détermination de l'échéance d'un billet à ordre payable à un certain délai de vue (ex : à trois mois de vue, je paierai…)

5) *Indication du lieu où le paiement doit s'effectuer* : le lieu de création du billet à ordre est réputé être le lieu du paiement ainsi, en même temps, que le domicile du souscripteur (*art. L. 512-1, III C. com*).
6) Il est aussi important d'indiquer *la date et le lieu où le billet est souscrit* ;
7) La *mention du bénéficiaire* : en principe, il n'est pas possible de créer un billet à ordre au porteur, et la mention du nom de bénéficiaire est exigée dans un billet à ordre, dont l'absence est sanctionnée par la nullité cambiaire[193].

360. Cependant la jurisprudence a décidé autrement, ce qu'elle a épargné le titre irrégulier de la nullité prévue par la loi, en considérant que lorsque le souscripteur émettait le billet à son propre ordre ; par ce fait, il confère à la banque la qualité de bénéficiaire en endossant le billet au profit de celle-ci[194]. Ainsi dans une autre décision jurisprudentielle, la Cour d'appel de Renne, dans un arrêt en date de 14 décembre 2007, le juge a retenu que si le billet ne comporte pas la mention du nom du bénéficiaire, il vaut comme billet au porteur[195]

361. Enfin, la *signature du souscripteur* est obligatoirement manuscrite (comme celle de l'accepteur, non du tireur). Ici nous reprochons au législateur français l'exigence d'une signature manuscrite. Cette mention de signature manuscrite

[193] Le billet au porteur ou le billet en blanc n'indiquant pas le nom du bénéficiaire ne peut avoir la valeur de billet à ordre, mais établit la créance contre le souscripteur dans les termes du droit commun : solution rappelée par Com. 1er mars 1994, *Bull*. no95.
[194] Com. 13 sept. 2011, no10-19.963, *Bull.* no 129; *D*. 2011. 2269, n. Delpech; *JCP G* 2011.1750, n. Lasserre Capdeville; *Gaz. Pal.*, 28 oct. 2011. 31, n. Houin-Bressand ; *Banque et Dr*. nov. 2011. 15, obs. Bonneau ; *Dalloz* actualité 22 Sept. 2011 ; *RD bancaire et fin*. Nov.-déc. 2011, obs. Crédot et Samin)
[195] Rennes, 1er ch. B, 14 déc. 2007, *RG* no 06/07107, Basle c/ Credit mutuel de Rohan Réguiny, *Juris-Data* no 357288.

obligatoire qui se trouve incompatible avec le régime des billets à ordre internationaux et la signature électronique que le commerce international a reconnus depuis plus qu'une dizaine d'années.

362. Si le titre ne respecte pas l'ensemble de ces exigences formelles, il ne vaudra pas comme billet à ordre. Toutefois, à l'imitation des solutions retenues pour la lettre de change, le billet à ordre incomplet pourra valoir comme preuve de l'engagement de droit commun du souscripteur, ou même comme un billet au porteur non soumis aux articles *L. 512-1* et suivants du Code de commerce[196].

B. Exigences de fond du billet à ordre

363. Concernant les conditions de fond, les exigences relevant du consentement, de l'objet et la cause de l'émission d'un billet à ordre sont identiques à celles imposées pour une lettre de change. La seule réserve c'est que le signataire d'un billet ne contracte pas nécessairement un engagement de nature commerciale puisqu'il ne s'agit pas forcément d'un acte commercial par la forme (comme étant le cas avec la lettre de change) et, par voie de conséquence, la capacité requise pour l'accomplissement d'un acte de commerce n'est pas exigée[197].

364. Ainsi les questions qui se posent dans une lettre de change en tant qu'acte de commerce n'auront pas lieu dans un billet à ordre. Par exemple la question relevant de la souscription d'un effet pour le compte d'un incapable est liée à la nature de la lettre de change, ce qui n'existe pas pour le billet à ordre.

365. Il convient aussi de rappeler que, comme nous avons signalé dans la lettre de change, l'engagement du souscripteur d'un billet à ordre est nul s'il est entaché d'un des vices mentionnés à l'*article 1109 du code civil*[198].

[196] Rouen, 14 juin 1963, *D*. 1963.636 ; *Banque* 1963.866, obs. Marin, V. Ss n°517.
[197] J. Stoufflet, *Op. Cit.*, n° 154.
[198] En ce sens pour l'aval d'un billet à ordre : Renne, 1e ch. B, 22 juin 2006, IV, 3467.

366. En ce qui concerne la cause du billet à ordre, la théorie de la provision n'existe pas dans un billet à ordre. Dans ce dernier, le souscripteur s'engage lui-même à payer le montant, ce qui signifie que cet engagement trouve sa cause dans le rapport fondamental qui lie le souscripteur au bénéficiaire.

367. Si le souscripteur désire se libérer de son engagement envers le bénéficiaire, il lui incombe de prouver l'absence de cause[199], sachant que l'absence de cause est inopposable à un porteur de bonne foi du billet.

368. Quant à la capacité, les dispositions relatives à la lettre de change s'appliquent au billet à ordre d'après le texte de l'*art. L. 512-4 du Code de commerce* qui renvoie, en cas de nullité du billet à ordre pour incapacité du souscripteur, aux dispositions de l'*art. L. 511-5* du même code sur le principe de l'indépendance des signatures dans un engagement cambiaire.

369. D'ailleurs, il faut préciser que des efforts sont aboutis en matière d'unification des règles de droit, en prenant acte de l'existence de principes communs à l'ensemble des effets de commerce. Citant par exemple la Commission des Nations Unies pour le droit commercial international (*CNUDCI*) auprès de qui une équipe de recherche était dévouée pour l'uniformisation du régime de la lettre de change et du billet à ordre au plan mondial.

370. Bien que ces efforts aient abouti à des textes importants qui servent dans le commerce international, l'ambition unificatrice qui les motivait n'a pas encore complètement abouti. Il en résulte qu'à côté des règles uniformes issues du droit conventionnel, les règles de conflit de lois du droit international privé ont encore vocation à s'appliquer.

371. **– Conclusion intermédiaire** – Outre les instruments financiers de mobilisation de créance, les 'documents transférables électroniques' peuvent être sous forme d'instruments financiers de garantie de créance.

[199] Paris, 14e ch. B, 26 sept. 1997 : D. 1997, inf. Rap. O.221. – Paris 3e ch. C, 20 Janv. 1995: *D.* 1996, *somm.* P. 34, obs. Cabrillac).

PARAGRAPHE II : INSTRUMENTS FINANCIERS DE GARANTIE DE CRÉANCE : WARRANTS ET LES RÉCEIPISSÉS D'ENTREPÔT (« LES DOCUMENTS TITRES »)

I. Notion de warrant-gage.

372. Il s'agit d'une variété de billet à ordre dont le paiement est garanti par un gage constitué sur des marchandises déposées dans un magasin général ou des marchandises que le souscripteur s'engage à conserver chez lui. Ainsi la particularité du warrant-gage est de réunir dans le même titre la promesse de payer à court terme une somme d'argent et la mise en gage d'un ou de plusieurs biens meubles corporels.

373. Ici le warrant-gage se diffère d'un billet à ordre classique. Bien qu'il s'agit d'un effet de commerce par détermination de la loi (*C. com., art. L. 522-35*), la fonction du titre consiste essentiellement à garantir un emprunt : c'est que l'émission de warrant garantit le plus souvent le remboursement d'un prêt ou d'une ouverture de crédit.

374. Le warrant présente un avantage par rapport au billet à ordre, c'est qu'il mobilise une créance garantie par une sûreté c.-à-d. que la constitution de gage se trouve intégrée dans le mécanisme du titre.

375. En conséquence, le warrant doit obéir à deux régimes juridiques différents ; d'une part en tant que billet à ordre il doit répondre, en règle générale, au régime du billet à ordre ; d'autre part en tant que gage, il obéit au régime de droit commun en matière du gage.

376. Il parait inévitable d'admettre le fait d'avoir cette sûreté dans le titre implique des règles particulières qui modifient la portée des obligations du souscripteur et les voies de recours cambiaires dont bénéficie le titre en tant que billet à ordre.

377. Le warrant, en tant que gage, est un écrit qui relève de l'article 1108-1 du Code civil et pourrait donc être conclu par voie électronique mais il tombe sous le coup des exceptions prévues par l'*article 1108-2* du même Code et ne peut donc être établi par voie électronique que s'il est constitué par une personne pour les besoins de sa profession.

378. Il est ici important de souligner qu'il ne faut pas confondre le 'warrant-gage' faisant l'objet de la présente section avec le 'warrant financier' qui ne porte pas la même signification ; ce dernier est défini comme un instrument financier conférant à son titulaire la faculté d'exercer une option d'achat (*call warrant*) ou de vente (*put warrant*) sur un élément sous-jacent de nature diverse, tels des valeurs mobilières, paniers ou indices de valeurs mobilières, devises, taux d'intérêt, matières premières, etc. [200]

379. - *Endossement du warrant* - Aux termes de l'*article L.522-26 du Code de commerce*, les récépissés et les warrants peuvent être transférés par voie d'endossement, quoi qu'ils soient ensemble ou séparément. Si le récépissé-warrant est endossé sans être détaché, il y a transfert de la propriété de la marchandise. Si le warrant est endossé seul, il y a constitution d'un gage sur les marchandises.

380. Tant que le warrant est un document titre qui représente des biens mobiliers, il ne constitue un effet de commerce et ne devient un véritable billet à ordre qu'à partir du moment où il fait l'objet d'un premier endossement. Ce premier endossement ne constitue pas uniquement une simple opération de transmission du titre mais c'est le moment de la création de warrant en tant que billet à ordre.

381. Ainsi l'endossataire d'un warrant-gage bénéficie de plus qu'une simple transmission de créance. Il s'agit d'une singularité de warrant puisqu'il présente un titre à double nature : il rend l'endossataire créancier du montant inscrit sur le

[200] HOVASSE (H.), "*Fasc. 2030 : Warrants financiers ", JurisClasseur Banque - Crédit – Bourse*, 1er Août 2012.

titre et qu'il transmet à celui-ci le droit de gage qu'il constate, lorsque le warrant est à la fois un effet de commerce et une sûreté.

382. Les conséquences de cette double nature du 'warrant-gage' ne sont pas toujours favorables car ça risque de créer un conflit de lois, c'est que le même titre détient deux façades, l'une sous forme d'un effet de commerce, l'autre relative au gage.

383. D'une part, les conflits de lois soulevés à propos du warrant par rapport à son rôle en tant qu'effet de commerce se posent de la même manière lorsque nous avons envisagé la différence entre la lettre de change et le billet à ordre.

384. Il est regrettable de savoir que bien que le warrant soit un effet de commerce, il n'est pas soumis aux règles uniformes des Conventions de Genève ; c'est que leur champ d'application est limité exclusivement aux lettres de change et aux billets à ordre; aucune disposition particulière ne vient unifier son régime ou fixer de règle de conflit de lois particulière le concernant : le droit international privé commun a donc vocation à régir le warrant dans son entier.

385. Tant que le statut juridique de warrant échappe à la loi uniforme ; en droit français, il est son fondement juridique dans une ancienne ordonnance datée de 6 aout 1945, puis elle fut modifiée par les dispositions de la loi du 28 mai 1858. Depuis la mise en application de l'ordonnance du 18 septembre 2000, les dispositions de l'ordonnance de 1945 ont été intégrées dans le texte du Code de commerce (les *articles L. 522-24* et suivants[201]).

386. D'autre part, dans sa fonction en tant que gage, le warrant donne naissance à d'autres conflits de lois qui s'articulent autour de la marchandise gagée et font donc intervenir la *lex rei sitae*[202]. le warrant se voit en principe appliquer la "*lex rei sitae*" (' La loi de la situation de la chose'). Ce terme qui gouverne le gage sur les meubles. Dans ce sens en droit international privé, la loi française est

[201] Le Cannu (P.), Granier (T.), Routier (R), *Op. cit.*, n° 502.
[202] THOMAS (V.), *Fasc. 566-20 : Effets de commerce. - Lettre de change et billet à ordre. – Warrant ; JurisClasseur Droit international,* 30 Octobre 2002, n°131.

"seule applicable aux droits réels dont sont l'objet les biens mobiliers situés en France".

387. La détermination de la *lex rei sitae* compétente ne présente ici grande difficulté :

- d'une part, la marchandise warrantée n'a pas, par hypothèse, vocation à changer de situation ;
- d'autre part, dans la mesure où elle a la nature de bien corporel, la situation matérielle de cette marchandise est fixée avec certitude. Tout conflit relatif à la détermination de la loi de situation est par conséquent exclu ;

388. Pourtant, en tant que sûreté réelle conventionnelle le warrant est rattrapé par la question qui porte sur le domaine respectif de la *lex rei sitae* et de la loi du contrat qui en est à l'origine ; qu'il faut distinguer entre le droit réel lui-même et la cause lui donnant naissance.

389. Il y a ainsi cumul des deux lois : la loi du contrat qui détermine si la sûreté a un fondement valable, puis la loi de la situation dira si ce type de sûreté peut exister. C'est de la sorte que les conditions d'existence de la sûreté doivent être vérifiées, la *lex rei sitae* ayant ensuite vocation à régir exclusivement les effets de la sûreté, à savoir les prérogatives du créancier sur la chose ainsi que les causes d'extinction de la sûreté.

II. Formes de Warrant-gage

390. Selon le type de warrant, le gage porte sur des marchandises déposées dans un magasin général (warrant avec dépossession) soit sur certaines formes de marchandises, limitativement énumérées par des textes particuliers, restant en la possession du constituant du gage (warrant sans dépossession).

A. Warrant avec dépossession

391. Les warrants avec dépossession sont aussi appelés les ‘warrants des magasins généraux’ ; ils sont des effets de commerce garantis par un gage portant sur des marchandises déposées dans un magasin général[203].

392. Un magasin général est un entrepôt dans lequel des industriels, des commerçants, des agriculteurs ou des artisans peuvent déposer des matières premières, des marchandises, des denrées ou des produits fabriqués. Ce magasin général délivre au déposant qui en fait la demande un titre appelé récépissé-warrant. C’est l'exploitant (personne physique ou société) de ces entreprises privées, ayant la qualité de commerçant, qui est habilité à délivrer aux déposants ces récépissés warrants.

393. Ce titre ne constitue pas un effet de commerce, il représente uniquement les marchandises déposées. Un récépissé d’entrepôt négociable est un document formant titre qui représente l’obligation de l’exploitant d’entrepôt de remettre des marchandises conservées dans l’entrepôt au porteur du récépissé. Les deux parties du titre peuvent être séparées : le récépissé qui donne droit à récupérer les marchandises n’est pas un effet de commerce ; le warrant, de son côté, s’analyse en un billet à ordre à statut particulier.

B. Warrant sans dépossession

394. Il existe plusieurs formes de warrant sans dépossession relevant de certains domaines d’activités :

1) Warrant agricole : il s’agit d’*un titre par le truchement duquel un agriculteur en même temps qu'il s'engage à payer une somme déterminée, confère au bénéficiaire ou aux porteurs successifs sur les biens de son exploitation, un gage sans dépossession*[204]. Le warrant agricole doit être constitué soir par

[203] Patrice Bouteiller, *Fasc. 765 : Gage Warrant*, 6 Avril 2016, *JurisClasseur Banque - Crédit – Bourse, n°111.*
[204] Patrice Bouteiller, *Op. cit., n°112.*

un agriculteur soit une société coopérative agricole ou d'une société d'intérêt collectif agricole (SICA)[205]. *(C. rur., art. L. 342-1[206]).*

2) Warrant industriel : cette sûreté était destinée à financer les matières utiles à la défense nationale et a été étendu par la suite, à des produits civils[207] ; le warrant industriel est devenu une sûreté en voie de disparition et n'est plus pratiquée aujourd'hui.

3) Warrant pétrolier : le warrant pétrolier a pour fonction d'autoriser les compagnies pétrolières à constituer des gages sur les stocks de pétrole. Le pétrolier doit maintenir le stock en valeur et en quantité à un niveau égal à ses engagements *(C. com., art. L. 524-16),* faute de quoi le porteur du warrant peut le mettre en demeure de rétablir le stock ou de le payer immédiatement. Cette sûreté est aujourd'hui ignorée de la pratique en raison de sa lourdeur et de son manque d'efficacité[208].

III. Conditions de validité de warrant-gage

395. Un warrant, comme tout autre effet de commerce, doit répondre à certaines conditions de forme (A) et de fond (B).

A. <u>Conditions de forme</u>

1) Mentions obligatoire.

396. Il s'agit ici de certaines mentions obligatoires prévues à l'article *L.522-24 du Code de commerce* : les unes doivent figurer au recto du titre ; les autres au verso : Au recto, le titre doit porter les mêmes mentions que le récépissé

[205] Patrice Bouteiller, *Op. cit., n°113.*
[206] Code rural et de la pêche maritime, version consolidée au 3 décembre 2016. [En ligne : https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071367].
[207] Patrice Bouteiller, *Op. cit., n°120.*
[208] Patrice Bouteiller, *Op. cit., n°121 et 122.*

constatant le dépôt dans le magasin général[209]. Aux termes de l'article *L.522-24 C.com* sont obligatoire les mentions suivantes : *le nom, profession et domicile du déposant, la nature de la marchandise et les indications propres à en établir l'identité et à en déterminer la valeur.* Bien qu'il ne soit pas inclus dans la liste ci-dessus, il est important de mentionner dans le titre la date du dépôt et la signature de l'exploitant.

397. Quant aux mentions qui figurent au verso du titre, il vaut remplir la clause suivante: « *Bon pour transfert du présent warrant à l'ordre de M…, demeurant à…, pour garantie de la somme de… payable le…* », date et signature.

398. De cette reformulation, nous saisissons l'exigence de cinq mentions qui sont : (1) la dénomination « warrant » (2) les noms et (3) domicile du créancier, (4) le montant de la créance garantie et (5) la date de l'échéance.

399. L'omission de l'une de ces mentions au verso du titre entraine la nullité du titre en qualité de warrant. Lorsque l'omission porte sur la date d'échéance, nous appliquons le texte de l'article *L. 512-1, II du code de commerce* qui répute payable à vue un billet à ordre qui n'indique pas la date d'échéance.

400. De même, l'omission d'une des mentions qui figurent au recto doit entraîner la nullité du titre en tant que warrant, mais le titre peut conserver la valeur d'un billet à ordre si les mentions obligatoires du verso sont complètes[210].

2) Mentions facultatives.

401. Il est possible de porter sur un warrant d'autres mentions facultatives ; en fait ce sont les mêmes mentions sur une lettre de change, à l'exception des clauses relatives à l'acceptation.

402. - *Clause non à ordre* - Cette clause non à ordre qui implique que le warrant doit être transmis par la voie de la cession de créance. En fait le législateur

[209] Patrice Bouteiller, *Op. cit., n°111.*
[210] V. P. LESCOT et R. ROBLOT, *loc. cit.* ; R. ROBLOT, *loc. Cit.*

français ne prévoit pas expressément la clause non à ordre dans la liste des mentions obligatoires, mais il a admis que le warrant peut être transmis par endossement. Il en résulte que l'absence de la clause sur le titre n'empêche pas la transmission par endossement.

403. Pourtant, le souscripteur peut avoir intérêt, pour son crédit en particulier, à ne pas voir le titre souscrit par lui passer entre les mains d'un trop grand nombre de personnes. Il lui sera donc possible de porter sur le titre le terme « non à ordre » ou toute autre formule équivalente pour empêcher la transmission du titre par endossement. Cette clause a été déclarée valable pour la lettre de change, et il n'y a pas de raison de le refuser pour le warrant. Nous revenons ainsi au texte de l'article *L. 511-8 du Code de commerce* qui prévoit dans cette hypothèse de « non à ordre » que le titre ne sera transmissible que « *dans la forme et avec les effets d'une cession ordinaire* ».

404. - *Clause portant dispense de protêt* - Le protêt est l'acte dressé par un huissier ou un notaire qui constate le refus de paiement à l'échéance ou le refus d'acceptation d'un effet de commerce par le débiteur.

405. La validité de cette clause dont le recours est accepté dans une lettre de change, ne reconnait la même aisance en matière de warrants. En France la doctrine est partagée pour accepter la clause dans un récépissé d'entrepôt[211]. Pourtant ce problème ne paraît donner lieu à aucune jurisprudence et la clause semble rarement employée en pratique.

406. Elle ne saurait avoir en tout cas qu'une utilité limitée, puisque la vente de la marchandise, pour refus de paiement, doit être obligatoirement précédée d'une sommation adressée au débiteur. Elle ne peut avoir d'intérêt que pour les recours du porteur non payé contre les endosseurs du titre.

[211] P. LESCOT et R. ROBLOT, *Les effets de commerce*, t. 2, 1953, n°840.

B. Conditions de fond.

407. Le warrant présente la particularité qu'il s'agit d'un effet de commerce réservé à certains professionnels. D'après l'article *L. 522-1 du code de commerce,* seuls peuvent accéder aux services des magasins généraux et donc recourir au warrant les industriels, commerçants, agriculteurs ou artisans.

408. Ainsi toute autre personne qui ne détient pas la qualité requise par la loi d'après l'*article L. 522-1* est de plein droit privé de la possibilité d'émettre un warrant. Aux termes de l'*article L.522-1 du Code de commerce*, le warrant porte sur des matières premières, des marchandises ou des denrées ou produits fabriqués. Il est d'ailleurs important de souligner que le warrant repose sur la mise en gage des stocks ; il est ainsi exclu toute mise en gage de matériel.

409. D'après une étude effectuée par le groupe de travail auprès de la Commission des Nations Unies, les 'documents transférables électroniques' ont connu beaucoup de succès au niveau international. Les récépissés d'entrepôt électroniques sont considérés comme les instruments les plus utilisés dans les pays en développement, étant un moyen efficace de fournir un financement aux agriculteurs et de contribuer ainsi à long terme à asseoir la sécurité alimentaire sur une base plus prévisible et durable[212].

410. En fait Les travaux réalisés par la *CNUDCI* dans ce domaine ont notablement participé à améliorer les pratiques dans les secteurs utilisant actuellement des documents transférables électroniques, et créeront un environnement dans lequel d'autres secteurs pourraient commencer à y recourir[213].

411. Dans les économies agricoles, les récépissés d'entrepôt électroniques permettront d'accroître le financement sur les marchandises entreposées[214]. Ceci s'explique par les avantages que présentent les récépissés électroniques sur les

[212] GABRIEL (H.), *"Warehouse Receipts and Securitization in Agricultural Finance", Revue de droit uniforme*, 2012, p. 369.
[213] Rapport de la Commission des Nations Unies pour le droit commercial international, Groupe de travail IV, Vienne, 29 octobre-2 novembre 2012, [En ligne: A/CN.9/WG.IV/WP.119 P.13, n°48]. .
[214] Henry Gabriel, *Op. Cit.* p.102.

récépissés papier ; ces avantages retirés de l'expérience des marchés agricoles nationaux où des récépissés d'entrepôt électroniques ont été utilisés.

412. L'utilisation des récépissés d'entrepôt électroniques réduit considérablement le coût des opérations, avec une meilleure transférabilité, accompagnée d'une plus grande sécurité pour le porteur.

413. Pour les producteurs agricoles, cela représente une augmentation claire des avantages découlant de l'utilisation des récépissés d'entrepôt, à savoir un meilleur accès au crédit et à des sommes plus importantes, la capacité de répondre à différents niveaux d'offre et de demande dus aux fluctuations du marché, et la capacité de vendre en gros et donc de réaliser des gains supplémentaires grâce au volume de vente. Les acheteurs y gagnent également car ils peuvent acheter de plus gros volumes et réguler la qualité des marchandises.

414. Tous ces avantages indiquent l'importance des récépissés d'entrepôt électroniques, surtout dans les économies agricoles en développement où ils ne sont pas très répandus actuellement.

415. Citons ici quelques exemples pour montrer le succès international des récépissés d'entrepôt électronique. D'abord, en Inde, il y a le texte de l'*article 11 de la Loi indienne sur l'entreposage* (*Warehousing (Development and Regulation) Act*) de 2007 qui prévoit explicitement l'utilisation de récépissés d'entrepôt sous forme électronique[215]. Toutefois, l'*article 2 du règlement de 2011 sur l'Autorité de développement et de régulation de l'entreposage* en Inde [216] (Récépissés d'entrepôt négociables) exclut actuellement les récépissés d'entrepôt négociables sous forme électronique.

416. Au Brésil, le système juridique actuel a mis au point la possibilité d'utilisation des certificats de dépôt et warrants agricoles sous forme

[215] La loi est entrée en vigueur le 25 octobre 2010 (on peut en trouver le texte intégral à l'adresse http://www.prsindia.org/uploads/media/vikas_doc/docs/acts_new/1199087479_THE_WAREHOUSING__DEVELOPMENT_AND_REGULATION_ACT_2007.pdf).
[216] Le texte intégral du règlement est disponible à l'adresse http://wdra.nic.in/.

électronique dans le secteur agricole afin de commercialiser les stocks déposés dans les entrepôts.

417. En Afrique, le développement de systèmes de récépissés d'entrepôt est devenu un moyen important d'améliorer la performance des systèmes de commercialisation de produits agricoles et les récépissés d'entrepôt électroniques deviennent populaires dans certains États d'Afrique. La *Proclamation n° 550/2007 sur la Bourse éthiopienne des marchandises* (portant création de la Bourse) prévoit la mise en place d'un système de récépissés d'entrepôt[217] ; et des régimes similaires existent en Afrique du Sud, au Ghana et en Ouganda. Par exemple, en 2004, le SAFEX (*South African Futures Exchange*) a annoncé qu'il accepterait des récépissés d'entrepôt aussi bien électroniques que sur papier pour le règlement de futurs contrats[218].

418. L'utilisation de documents transférables électroniques aux États-Unis remonte à près de 20 ans, avec une réglementation fédérale prévoyant l'utilisation de récépissés d'entrepôt électroniques dans le secteur du coton[219].

419. Les systèmes de récépissés d'entreposage dans le domaine de commercialisation du coton existent depuis longtemps[220]. D'après ce système,

---

[217] Créés par la loi n° 11.076/04, les certificats de dépôt et warrants agricoles sont des instruments de crédit liés à la production déposée dans des entrepôts. Les certificats représentent la promesse de livraison des marchandises déposées et les warrants accordent le droit de rétention sur les marchandises décrites dans les certificats. Ces instruments sont corrélatifs, en ce sens qu'ils sont émis au même moment et se réfèrent au même lot de marchandises. Ils sont émis par le dépositaire des marchandises qui appartiennent aux propriétaires des stocks ou aux acheteurs successifs des instruments. Ils doivent être enregistrés et conservés dans une entité habilitée par la Banque centrale. Dès ce moment, la négociation des instruments devient nécessairement électronique. Les warrants permettent au porteur de constituer une garantie sur le produit pour obtenir un prêt bancaire, alors que les certificats lui permettent de vendre les marchandises sans qu'aucune taxe ne soit due jusqu'à ce que le propriétaire des instruments, en tant qu'agent économique, ne souhaite effectivement utiliser le produit stocké pour la transformation ou la vente.

[218] Sarel F. du Toit, *Reflections on Bills of Lading and Silo Receipts used in the South African Futures Market*, 2 *Journal of International Commercial Law and Technology 3 (2007) 105; Gideon Onumah*, *Promoting Agricultural Commodity Exchanges in Ghana and Nigeria: A Review Report*, Rapport établi pour la CNUCED, p. 8 et 9; Gideon Onumah, *Implementing Warehouse Receipt System in Africa – Potential and Challenges*, établi pour le Quatrième colloque africain sur la politique des marchés agricoles, Malawi, 6-7 septembre 2010, actes disponibles à l'adresse : http://www.aec.msu.edu/fs2/aamp/sept_2010/aamp_lilongwe-onumahwarehouse_receipt_systems.pdf ; *Ghana Grains Council Warehouse Receipt System Rules and Regulations*, article 26-3: "*GGC Warehouse Receipts shall be paper or electronic documents*" ("Les récépissés d'entrepôt du Conseil des céréales du Ghana sont des documents sous forme papier ou des documents électroniques").

[219] Code des règlements fédéraux (United States Code of Federal Regulations), titre 7: agriculture, sect. 735: Regulations for the United States Warehouse Act (réglementation concernant la Loi sur les entrepôts).

un récépissé d'entreposage est établi au nom d'un déposant (un agriculteur, un groupe d'agriculteurs, un transformateur ou un négociant) pour attester qu'il ou elle a déposé un produit de base donné, dans les quantités et de la qualité indiqués, à un endroit donné. Le titulaire du récépissé peut le donner en gage à un prêteur (la marchandise déposée servant de garantie pour le prêt) ou le transférer à un acheteur (par le biais d'une vente). L'exploitant de l'entrepôt ou le tiers détenteur (*collateral manager*), qui détient les stocks, garantit la livraison contre le récépissé, et devrait compenser toute perte de valeur dû au vol, à l'incendie ou à d'autres catastrophes. Ici les acteurs principaux du système des récépissés d'entreposage sont les déposants, l'exploitant de l'entrepôt ou le tiers détenteur, et les prêteurs ; et que leurs rôles, responsabilités et bénéfices se varie selon que le système est réglementé ou non. De toute manière, le secteur du coton est au niveau international, est l'un des mieux régi par des règles contractuelles

420. En conclusion. Les conditions classiques nécessaires à l'élaboration de ces effets de commerce se transposent intégralement aux documents électroniques qui doivent en adopter toutes les caractéristiques. Mais un problème plus épineux se pose, celui de la preuve de la validité de la signature et de la sécurisation des données.

[220] Guide de l'exploiteur de coton – Centre du Commerce International, [En ligne : http://www.guidedecoton.org/guide-de-coton/en-quoi-consistent-les-systemes-de-recepisses-dentreposage/].

CONCLUSION DU CHAPITRE I

421. La liberté de communication est un principe fondamental pour pouvoir faire circuler les ‘documents transférables électroniques’ sur le web; au niveau national, cette liberté est reconnue et consacrée par la loi du 29 juillet 1881 sur la liberté de la presse, la DDHC (art 11), puis intégrée dans les préambules de la constitution de 1946 et de 1958.

422. Pourtant cette liberté ne doit pas porter atteinte au respect de la vie privée ; la protection des données personnelles évolue dans le temps. La preuve en est de la loi du 6 août 2004, transposée de la Directive européenne 95/46/CE du 24 octobre 1995, puis du Règlement européen 2016/679 du 27 avril 2016 ; ce dernier vise à promouvoir l’utilisation de l’outil informatique, tout en accordant la protection appropriée aux données à caractère personnel.

423. Les législateurs français et européen ont adapté leurs régimes juridiques respectifs sur les effets de commerce classiques, pour pouvoir intégrer l’équivalent de ces derniers sous forme électronique. Au fur et à mesure de notre présentation des critères de validité qui gouvernent la lettre de change, les billets à ordre et les récépissés d’entrepôt, nous constatons que les même critères sont susceptible d’être appliqués aux ‘documents transférables électroniques’.

CHAPITRE II

LA CONCLUSION DU ‘DOCUMENT TRANSFÉRABLE ÉLECTRONIQUE’

424. Comme tout acte juridique, les documents, revêtant une valeur probante et contraignante, sont soumis à une signature manuscrite s'il s'agit d'un document papier ou à une signature électronique lorsque l'acte est électronique lui-même.

425. La signature représente le processus final pour achever la dématérialisation d'un document électronique en préservant ses caractéristiques juridiques, voire son authenticité.

426. Afin d'atteindre cet objectif, il est inévitable de caractériser le besoin d'avoir un réseau sécurisé permettant d'éviter que la valeur juridique du document ne soit remise en cause à l'occasion du défaut d'identification de l'une des parties de l'opération en question.

427. Lorsque nous atteignons cet objectif d'avoir un réseau efficacement sécurisé et d'avoir la régulation nécessaire pour garantir la fiabilité des signatures posées sur les documents partagés par voie électronique, nous parlons ainsi de la présomption de fiabilité de la signature électronique.

428. Cette présomption de fiabilité a été encouragée par le législateur européen qui établit ce principe afin de promouvoir l'utilisation des documents transférables par voie électronique.

429. Nous présentons dans un premier temps la notion de la signature électronique, ainsi que les moyens permettant à son identification et leur authentification. C'est ainsi que nous reconnaissons la signature cryptographique comme équivalent de la signature manuscrite (Section I). En deuxième temps, nous traitons le mécanisme de la cryptologie à clé publique pour protéger la signature électronique contre l'espionnage en ligne (Section II). Tous ces éléments de la signature électronique et de la cryptologie sont applicables aux effets de commerce et nécessaires non seulement à leur authentification mais à leur validité.

SECTION I : LA SIGNATURE ÉLECTRONIQUE : LE SUPPORT

430. La notion de signature électronique, et les différents procédés d'identification et d'authentification des documents électroniques, seront examinés avant d'aborder les règles de la preuve et la portée juridique de la signature sur la preuve **(Paragraphe I)**.

431. Dans un deuxième temps, nous envisageons les différents mécanismes de la cryptographie jusqu'à l'arrivée de l'informatique en nuage, et les règles juridiques qui les gouvernent en France et en Europe **(Paragraphe II**).

PARAGRAPHE I : CONSÉCRATION DE LA SIGNATURE CRYPTOGRAPHIQUE COMME ÉQUIVALENT DE LA SIGNATURE MANUSCRITE

432. La sécurisation des actes électronique est un défi (I), auquel répondent la mise en place de la signature électronique et différents systèmes de gestion électronique (II) ; nous parlerons ensuite de la confiance en l'identité numérique (III) pour aborder finalement les règles de la preuve et la présomption de fiabilité de la signature électronique (IV)

I. Défis de la sécurisation des actes électroniques

A. Notion d'écrit électronique

433. Il convient d'abord de préciser que lorsque nous avons recours à des écrits électroniques, cela reste subordonné à l'accord de volonté des parties sur l'emploi de cette forme; celle-ci, si elle ne peut, en principe, être refusée en raison de l'équivalence des formes écrites et électroniques, doit cependant être rejetée à chaque fois qu'il n'est pas établi que les parties possèdent tous les

équipements requis pour assurer la transmission et le déchiffrage de tels documents.

434. Avant la loi n° 2000-230 du 13 mars 2000, il a été reproché à plusieurs reprises au législateur français de ne pas prévoir de définition d'écrit électronique, et lorsqu'il n'y a pas de texte juridique pour déterminer sa signification, il ne serait pas reconnu comme moyen de preuve.

435. Pour remédier à cela, ont été révisées les dispositions des articles 1316-1 et 1316-4 du Code civil depuis l'entrée en vigueur de la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique[221].

436. Ces textes ont innové avec pour la première fois une définition de la notion d'écrit qui se présente comme : *"...une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission*" (C. civ., art. 1316) [222]. Une nouvelle définition qui propose simplement la notion de l'écrit, indépendamment de son support et de son mode de transmission.

437. Depuis la loi du 13 mars 2000, le législateur français a explicitement consacré le principe de la neutralité du support de l'acte juridique et a consacré l'écrit électronique. Au terme de l'article 1316-1 du Code civil, "*l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier (...)*". De plus, ce même principe a été mentionné implicitement dans le texte de l'article 1326 du Code civil ; car le législateur a modifié ce dernier par la loi n° 2000-230 du 13 mars 2000, article 5 dans le sens où il a supprimé la référence à l'écrit manuscrit.

438. En application de ces textes susmentionnés, nous constatons la dualité de l'écrit; la même notion d'écrit recouvre désormais deux modalités : l'écrit

[221] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JO du 14 mars 2000, p. 3968.
[222] Version électronique du Code civil consolidée au 9 octobre 2016, [En ligne : https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006437784&dateTexte=&categorieLien=cid].

"traditionnel" sur support papier et l'écrit "sous forme électronique". L'écrit électronique est soumis à certaines conditions, habituelles mais peu exprimées dans le monde du papier, pour être recevable et notamment, pour présenter la même force probante que l'écrit papier.

B. La dématérialisation de l'écrit

439. Le concept de dématérialisation consiste en ce que l'information est inscrite *ab initio* sur support informatique. Les données sont ici initialement créées sous format numérique.

440. Toutefois, la dématérialisation concerne tout aussi bien l'action par laquelle les données, sur support papier, sont transférées et/ou transformées en fichiers informatiques : les documents sont numérisés. Il s'agit ici de l'hypothèse selon laquelle les documents sont initialement créés sous format papier puis informatiquement reproduits ou copiés.

441. La question se pose ici de la possibilité de la dématérialisation des instruments de paiement et du droit cambiaire. Nous avons constaté que dans le passé *"le droit cambiaire était peu compatible avec les nouvelles technologies"*[223]. Le Professeur C. Lucas de Leyssac[224], a même évoqué *"l'incompatibilité entre la civilisation cybernétique - dématérialisée ou même virtuelle - et la tradition juridique française qui repose en matière de preuve, sur la prévalence d'un support matériel : l'écrit"*. Il est permis de penser que la réforme du droit de la preuve, alors même que tel n'est pas son objet initial, a remis en cause cette incompatibilité.

442. Deux situations doivent être nettement distinguées selon que nous envisageons l'impact de la réforme sur les effets de commerce dans leur forme traditionnelle, ou la création d'effets de commerce entièrement électroniques.

---

[223] Éric A. CAPRIOLI, *Droit cambiaire et signature électronique*, *LexisNexis*, *Communication Commerce électronique* n° 10, Octobre 2011, *comm.* 97. En ce sens, voir aussi T. Bonneau, note sous *Cass. com., 26 nov. 1996, op. cit. n° 7.*

[224] CA Orléans, 17 févr. 2011, n° 10/02082, Guy Tual c/ SAS Lafarge Bétons de l'Ouest : JurisData n° 2011-002558. En ce sens, voir aussi : *Le droit fondamental de la preuve, l'informatique et la télématique : Petites affiches 29 mai 1996, n° 65, p. 3.*

443. Concernant les ordres de paiement totalement dématérialisés ne revêtant pas la forme d'effets de commerce, le principe du consensualisme s'applique et permet une très large validation de ces procédés, indépendamment de la réforme du droit de la preuve[225].

444. Sur le formalisme juridique de l'écrit électronique, la pratique contractuelle est gouvernée par le principe du consensualisme, c'est-à-dire que la volonté suffit pour former un contrat. Le contrat est donc valable du seul fait de l'échange des volontés[226].

445. Par ailleurs, la validité de certains actes est conditionnée par une mention manuscrite de la part de la personne qui s'engage. L'article 1108-1 prévoit que lorsqu'une mention manuscrite est exigée « *de la main même de celui qui s'oblige, ce dernier peut l'apposer sous forme électronique si les conditions de cette apposition sont de nature à garantir qu'elle ne peut être effectuée que par lui-même* ».

446. Ainsi le texte de l'article 1108-1 du Code civil issu de la loi sur l'économie numérique établit une autorisation générale de la dématérialisation en acceptant l'établissement et la conservation d'un écrit sous forme électronique, sous respect des conditions prévues dans la loi.

447. Cette reconnaissance générale de l'écrit électronique peut aussi être énoncée de la façon suivante : à l'exception des actes dont la liste est fixée par la loi, la substitution d'une forme électronique à un acte sur papier est valide à condition que la forme électronique résultante dispose d'une force probante équivalente.

448. Pourtant nous entendons par l'usage d'un acte électronique un changement de forme de l'acte juridique, ce qui porterait, en théorie, atteinte à un grand principe du droit, qui est le formalisme juridique.

---

[225] Sur ce point *V.* M. Espagnon, *L'ordre de paiement émis sur Internet : RD bancaire et bourse n° 71, janv.-févr. 1999, p. 7.* En ce sens, voir Thierry Piette-Coudol, *Fasc. 80 : Les Collectivités Territoriales Face aux Technologies de l'Information et de la Communication*, *LexisNexis*, 24 Octobre 2014, p. 8 et s.

[226] En ce sens, voir : Luc Grynbaum, *Fasc. 10 : La Preuve Littérale - Dispositions générales - Écrit électronique*, *LexisNexis*, 19 Décembre 2011, mise à jour le 17 Juin 2016.

449. Le formalisme juridique est naturellement constitué de l'ensemble des formalités nécessaires à la formation d'un acte juridique donné. Les contraintes majeures relevant de ce dernier sont habituellement l'exigence d'un support papier, l'apposition d'une signature manuscrite et la présence de mentions obligatoires prévues par la loi.

450. À l'occasion de la dématérialisation, le formalisme juridique s'associe à un principe assez nouveau qui est le 'droit constant'. D'après les principes de techniques législatives, le fait pour un législateur de coordonner « à droit constant » consiste à rassembler et à ordonner dans un acte unique les règles existantes d'un ou plusieurs actes qui ont le même objet, sans avoir l'intention de créer de nouvelles règles. Cette méthode de coordination adoptée vise principalement à harmoniser les modifications successives qui sont apportées par des actes législatifs, sans pour autant créer de règles nouvelles.

451. Ainsi nous retenons qu'une caractéristique du droit, d'après ce principe susmentionné, est l'unicité des règles de droit portant sur le même objet, et que le droit ne change-t-il pas lors du passage du support écrit à la forme électronique. Cet aspect d'« unicité » fait partie des questions traitées dans la deuxième partie de la thèse.

452. Lorsque le document électronique est ainsi réalisé à droit constant, il est identique au document d'origine, mais sous une forme électronique, et qu'il faudra alors pratiquer le parallélisme des formes de la façon suivante :

- le support papier est remplacé par la forme électronique (*C. civ., art. 1108-1*) ;
- la signature manuscrite est remplacée par une signature électronique (*C. civ., art. 1316-4*);
- les mentions obligatoires sont présentes dans la forme électronique comme sur le support papier (*C. civ., art. 1108-1*).

453. Sur la notion de sécurisation des actes électroniques, l'acte, devenu électronique, est susceptible d'être transporté par plusieurs vecteurs de télécommunication, aujourd'hui par Internet. Comme ces vecteurs ne présentent pas le même degré de sécurité de base, il est nécessaire de recourir à des

mesures de sécurisation afin que l'acte dématérialisé atteigne le même niveau de sécurité que le papier (conservation des attributs juridiques)[227].

454. Afin de parvenir à une dématérialisation réputée acceptable sur le marché, il faut rassurer le simple utilisateur sur l'intégrité des procédés mis en œuvres pour contrôler la transaction exécutée par voie électronique ; comme nous avons traité dans le premier chapitre les critères de validité à respecter pour reconnaitre un effet de commerce en version électronique, il faut aussi que ce dernier, étant la forme dématérialisée de son équivalent papier, soit sécurisé pour lui conserver ses attributs juridiques ; ce n'est qu'à cette condition que nous pourrons accorder au document électronique la même protection qu'à un document sous forme manuscrite ; et cette sécurisation juridique, une fois acquise, s'étend à tous les stades du cycle de vie de la forme électronique.

455. A cet égard, Madame Elisabeth JOLY-PASSANT retient que l'*efficacité d'une preuve tient le plus souvent à la sécurité offerte par son support, de sort que les modalités d'efficacité probatoire de la preuve littérales mais aussi du support du moyen de preuve lui-même*[228]. Il faut souligner qu'est seulement exigé un niveau de sécurisation minimal, car il n'est pas question de demander à l'électronique plus de garanties qu'au papier.

456. Un revirement de la pratique bancaire s'est produit suite à la dématérialisation de l'écrit ; en fait, nous devons distinguer deux axes majeurs qu'empruntera la dématérialisation de l'écrit en droit bancaire : d'une part, elle est riche de conséquences en matière d'effets de commerce ; d'autre part, la dématérialisation va modifier les pratiques utilisées, ou exigées, dans les relations entre les banques et leurs clients, en concernant un grand nombre de documents bancaires ; ainsi devrait-on, prochainement, assister à une diminution

[227] PIETTE-COUDOL (Th.), *Fasc. 80 : Les Collectivités Territoriales Face aux Technologies de l'Information et de la Communication*, *LexisNexis*, 24 Octobre 2014, n°35 et s.
[228] JOLY-PASSANT Elisabeth, *L'écrit confronté aux nouvelles technologies*, *L.G.D.J*, 2006, p. 380, n°847. Voir aussi GAUDRAT (P.), *Introduction, in Une Société sans papier ? Droit de la preuve et nouvelles technologies de l'information (rapport-cadre), La documentation Française*, 1990, p. 170.

majeure de la discordance observée entre le formalisme et les impératifs bancaires[229].

457. Le mouvement de la dématérialisation des documents a été anticipé par les juristes dans le passé ; dans sa remarque étude consacrée à la lettre de change relevée le Professeur Vasseur, dès 1975, a observé que le législateur pouvait créer la "lettre sans la lettre"[230]. Chose faite, grâce à la consécration de la dualité de la notion d'écrit : tantôt matérialisé dans sa forme traditionnelle, tantôt dématérialisé dans sa forme électronique[231].

458. Reprenons la définition classique de la lettre de change, s'agissant d'un "*'écrit par lequel le tireur donne mandat au tiré de payer à un tiers, le preneur ou bénéficiaire, ou à son ordre, une certaine somme à une époque déterminée*"[232], nous voyons bien dans cette définition que rien ne s'oppose à ce qu'un écrit soit un écrit électronique, bien au contraire. Il est dorénavant acceptable de fournir un document juridiquement opposable aux parties que ce soit un écrit manuscrit ou un écrit électronique.

459. Il paraît alors évident qu'il s'agit en fait d'une véritable révolution de la notion d'écrit. En effet, il résulte des termes mêmes employés par le législateur, et de l'unité de la notion d'écrit, qu'il faut admettre qu'à chaque fois qu'un écrit est exigé, que ce soit *ad probationem* ou *ad solemnitatem*, l'écrit électronique, accompagné d'une signature de même nature est désormais recevable au même titre que l'écrit traditionnel, sous la seule réserve de l'exigence d'une forme spéciale. La signature électronique va être traitée plus tard dans ce chapitre.

---

[229] V. J. Devèze, *À propos de la réforme du droit de la preuve : observations tirées du droit des instruments de paiement : Mélanges Michel Cabrillac*, 2000, p. 449 s. qui relève que "*Le formalisme direct, sanctionné par la nullité de l'acte, est un obstacle assurément redoutable lorsqu'il impose un écrit, par exemple pour protéger le consommateur encore que des adaptations aux exigences les plus fortes puissent être le fait de la pratique [LCR], du législateur [...], ou de la jurisprudence [...]"* ; Plus généralement : P. Villeroil, *La télétransmission confrontée au droit de la preuve - Un aspect de la banque à distance : Banque et droit* n° 63, janv.-févr. 1999, p. 22.

[230] M. Vasseur, *La lettre de change-relevé - De l'influence de l'informatique sur le droit* : *RTD com.* 1975, p. 203.

[231] En ce sens, voir François Guy TRÉBULLE, *L'incidence de la réforme de la preuve sur le droit bancaire, Revue de Droit bancaire et financier* n° 2, Mars 2000, étude 100010, n°2 et s.

[232] François Guy TREBULLE, *Ibid.*

460. Ce mouvement de dématérialisation de l'écrit dépasse certainement les vœux du législateur ; mais il s'inscrit parfaitement dans la logique communautaire qui vise à imposer l'égalité de traitement entre les formes traditionnelles et les formes électroniques propres à la société de l'information. Citons l'exemple de la lettre de change-relevée et le billet à ordre relevé qui témoigne de la pesée de l'informatique sur les opérations de banque, et ce n'est que l'une des nombreuses applications de l'informatique bancaire. La banque est "*la terre d'élection des opérations de masse qu'expliquent notamment la "bancarisation" des ménages, l'ouverture multipliée de comptes et la dématérialisation des moyens scripturaux ainsi que l'évolution de l'épargne vers les placements financiers avec l'accroissement du nombre de titres à gérer, la mondialisation des échanges économiques et les transferts internationaux de fonds*"[233]

461. D'une part, la lettre de change relevé est un moyen d'échanger des lettres de change de manière dématérialisée, un effet commerce dématérialisé qui circule sous forme de fichiers informatiques. Elle est créée à l'initiative du créancier (le tireur) qui l'envoie à sa banque afin que celle-ci l'adresse à la banque de son débiteur. La profession bancaire a créé la lettre de change relevé (LCR) pour simplifier les traitements de la lettre de change (et surtout réduire les coûts pour les banques puisque la lettre de change classique nécessite de nombreuses manipulations de papier) tout en conservant ses modalités et conditions juridiques[234]. La lettre de change-relevé magnétique ne repose pas sur un titre soumis aux conditions de validité de l'article L. 511-1 du Code de commerce, et constitue un simple procédé de recouvrement de créance dont la preuve de l'exécution relève du droit commun[235].

462. D'autre part, le billet à ordre relevé (BOR) relève, quant à lui, du support papier, car il concrétise un engagement de payer qui requiert la signature du souscripteur. Il est normalisé (NFK 11.080) et comporte toutes les mentions

[233] Jean-Pierre Deschanel, *Fasc. 440 : Lettre de change relevé (LCR) Billet à ordre relevé, jurisClasseur Banque - Crédit – Bourse*, 15 Juillet 1999, mise à jour le 27 Novembre 2015, n°1 s.
[234] Jean-Pierre Deschanel, *Op. cit*., n°19.
[235] Cass.com., 2 juin 2015, n° 14-13.775, FS-P+B, M. X c/ Banque populaire des Alpes *: JurisData* n° 2015-013154; *JCP E 2015*, 1466, note Rodriguez : *RD bancaire et fin. 2015, comm*. 179, obs. Francis-J. Crédot et Th. Samin.

prescrites par le Code de commerce (art. 183) et l'identification bancaire du souscripteur (RIB)[236].

463. Bien que le droit civil ait été bouleversé par cette évolution, celle-ci apporte une réponse innovante au lancinant problème des manipulations de papier et l'avancement du commerce électronique.

464. Une fois L'écrit électronique est considéré valide, il sera recevable comme preuve (C. civ., art. 1316-1) comme l'est l'écrit papier. Il possède la même force probante qu'un écrit papier (C. civ., art. 1316-3), et le juge réglera tout conflit éventuel de preuve en déterminant par tous moyens le titre le plus vraisemblable quel qu'en soit le support (C. civ., art. 1316-2).

465. En agissant de la sorte, la doctrine a assuré que l'écrit électronique *ad probationem* trouvait ses bases légales, tout en soulignant qu'il restait un vide à combler avec la question de l'écrit électronique *ad validitatem*.

466. Ce défi a été relevé et le cas de l'écrit électronique *ad validitatem* est résolu avec l'article 25 de la loi sur l'économie numérique n° 2004-575 du 21 juin 2004 (Journal Officiel 22 Juin 2008) qui a été transposé dans la loi en France, en créant le nouvel article 1108-1 dans le Code civil.

467. Le nouvel article 1108-1 du Code civil prévoit que "*lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique...*". L'article 25 de ladite loi balise ainsi le parcours du juriste ; celui-ci dématérialise d'abord si la base légale est suffisante, puis il revalide juridiquement la forme substituée en établissant l'identification et l'intégrité du substitut électronique.

468. La substitution d'une forme électronique à un support papier s'opère à droit constant. En l'absence d'obstacles formels à la dématérialisation, l'article 1108-1 C.civ se présente comme une autorisation générale de dématérialisation.

[236] Jean-Pierre Deschanel, *Op. cit.*, n°18.

469. Concernant la confidentialité de l'écrit électronique, dans les échanges électroniques, les fichiers et les messages sont transmis sans enveloppe, ce qui les rend plus accessibles aux indiscrets, aux curieux et autres pirates. Aussi, pour tous les réseaux de télécommunications, à plus forte raison pour Internet, les entreprises comme les particuliers présentent-elles une forte demande de confidentialité pour protéger les échanges commerciaux, stratégiques et concurrentiels.

470. Pourtant, rien dans le droit civil ou commercial appliqué à l'électronique ne traite d'une obligation de confidentialité. Il en est ainsi parce que la confidentialité est garantie par le secret qui est de mise dans les télécommunications.

471. Appliqué dès l'origine aux lettres et paquets confiés à la poste, le secret des correspondances s'est étendu aux télécommunications. L'assimilation a été renforcée par la *loi n° 91-646 du 10 juillet 1991* relative au secret des correspondances émises par voie de télécommunications[237]. Le principe est donné par l'article 2 de la loi en prévoyant que "*Le secret des correspondances émises par la voie des télécommunications est garanti par la loi*".

472. D'après l'article 1er de la loi précitée, le secret est absolu, et que les seules exceptions au secret sont des écoutes de deux types : les interceptions ordonnées par l'autorité judiciaire et les interceptions de sécurité faite par l'Administration sur autorisation du Premier ministre.

473. D'ailleurs, la protection des données personnelles peut dans certains traitements techniques exiger la confidentialité[238]. Au demeurant, l'importation, la fourniture ou l'usage de moyens cryptographiques assurant la confidentialité (chiffrement lourd) entre dans le cadre de la cryptologie réformé par la loi sur l'économie numérique et est susceptible de renvoyer au régime administratif de la déclaration ou de l'autorisation.

[237] Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, *Journal Officiel* 13 Juillet 1991.
[238] V. L. n° 2004-801, 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 35 : *Journal Officiel* 7 Aout 2004.

474. Le régime juridique de la confidentialité dans le commerce électronique est assez complexe et comporte plusieurs facettes qui doivent toutes être surveillées dans l'hypothèse des '*documents transférables électroniques*'. Il s'agit des déclinaisons suivantes de la confidentialité, en contexte papier ou électronique :

- confidentialité des échanges électroniques, garantie par la loi n° 91-646 du 10 juillet 1991 relative aux correspondances émises par voie de télécommunications;
- confidentialité des données personnelles pendant les transmissions ainsi que dans les traitements ultérieurs, sur papier ou sous électronique, garantie par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[239]

475. Du fait de la complexité de la technique à mettre en œuvre et de la réglementation à respecter, il est préférable en matière de commerce électronique de s'en remettre à des plates-formes dont les équipements présentent les moyens de confidentialité voulue par les textes.

[239] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *Journal officiel* du 7 janvier 1978 et rectificatif au *J.O.* du 25 janvier 1978.

II. Présentation de la signature et des systèmes de gestion des documents électronique

A. Notion de signature électronique.

476. Curieusement qu'il n'existe pas un texte de la loi pour définir le terme 'signature' ; en l'absence de définition légale, la signature peut se décrire en tant que graphisme original qui exprime de manière non équivoque la personnalité d'un individu et de son adhésion au contenu de l'acte[240].

477. En fait, le risque couru ici est que si la personne dénie la signature posée sur l'acte, la signature perd toute sa valeur et son existence, à moins de respecter la procédure de vérification d'écriture. Donc, il faut retenir précieusement cette dernière pour pouvoir satisfaire aux conditions de reconnaissance de la signature en cas de litige.

478. En principe, il existe plusieurs moyens, ou supports d'identification de la personne : badge, empreintes digitales ou même un fond d'œil, sous la seule condition que l'intéressé en accepterait l'usage. Ces outils servent évidemment à accorder plus de garanties qu'une signature imitable.

479. Nous saisissons une définition fonctionnelle de la signature qui a été publiée à l'Observatoire juridique des technologies de l'information (services du Premier ministre, 1991) ; d'après sa définition il s'agit de *« tout signe intimement lié à un acte, permettant d'identifier son auteur et traduisant sa volonté non équivoque de consentir à cet acte »*[241].

480. De cette définition, nous relevons l'exigence d'un lien existant entre le signe employé par le signataire et l'acte signé, permettant à son identification et qui reflète sans le moindre doute sa volonté réelle de consentir à l'acte.

---

[240] http://www.larousse.fr/dictionnaires/francais/signature/72699.

[241] *Du sceau numérique à la signature électronique*, sous la direction de C. DHENIN, *Vers une administration sans papier, Paris, La documentation Française*, 1996, p.96.

481. Parallèlement, lorsque nous sommes dans un contexte informatique, la signature numérique fait recours au cryptage qui sert à révéler l'identité et déterminera ainsi la volonté du signataire. Nous envisagerons la technique de cryptage en détail plus tard dans le présent chapitre.

B. Système de gestion des documents électroniques (GED) : L'échange de Données Informatisées 'EDI'

482. Pour automatiser le traitement de l'information dans l'optique du "zéro papier", s'est créée la notion de l'EDI ('*Electronic Data Interchange*', traduit en français : 'Echange de Données Informatisées').

483. L'EDI se définit comme *l'échange, d'ordinateur à ordinateur, de données concernant des transactions en utilisant des réseaux et des formats normalisés*. Autrement dit, dans des termes plus techniques, ce sont les informations issues du système informatique de l'émetteur qui transitent par l'intermédiaire de réseaux vers le système informatique du partenaire pour y être intégrées automatiquement.

484. Nous entendons par texte véritablement EDI les messages étant validés au cours des quatre stades: émission, expédition, réception du message dans le système informatique du destinataire, acceptation (distincte du simple accusé de réception).

485. Quant à la valeur juridique de l'EDI, la recommandation de la commission européenne de 19 octobre 1994 [242] a reconnu les messages EDI comme conséquence naturelle d'une confiance justifiée et accrue dans des techniques sans cesse améliorées et mieux maitrisées par les initiateurs de systèmes nouveaux.

[242] 94/820/CE: Recommandation de la Commission, du 19 octobre 1994, concernant les aspects juridiques de l'échange de données informatisées (Texte présentant de l'intérêt pour l'EEE).

486. Il est nécessaire d'avoir une coordination et une convergence d'effort dans les milieux professionnels, administratifs et juridictionnels afin de reconnaitre pleinement la valeur juridique de l'EDI.

487. Pour cela, il est absolument nécessaire de prendre en charges certaines initiatives, comme assurer la liaison entre les spécialistes du droit et de la télématique, les instances nationales publiques et privées, et les organisations dépendant des Communautés européennes ou de l'ONU. L'interaction de ces spécialistes et organisations d'orientations diversifiées est une solution satisfaisante pour franchir les obstacles jugés incontournables, et d'explorer des voies qui semblaient dans l'impasse.

488. De point de vue historique, l'EDI n'est pas vraiment un nouveau terme qui appartient à la dernière décennie, il est connu la première fois en France depuis 1987 ; il y avait même certaines applications qualifiées aujourd'hui d'"'EDI" qui étaient apparues dès 1980 dans le monde bancaire. La pratique de la lettre de change relevée magnétique est un exemple de l'utilisation de l'EDI dans le secteur bancaire.

489. Les avantages de l'EDI sont nombreux, nous pouvons citer principalement l'abaissement des coûts, l'accroissement d'efficacité des interventions d'organismes officiels, la diminution des délais d'acheminement ainsi que tous les mérites déjà reconnus à la gestion électronique de documents (GED)[243], dont l'EDI diffère radicalement par son degré de dématérialisation et d'automaticité interactive.

[243] La gestion électronique des documents (*GED* ou en anglais DMS pour *Document Management System* ou *EDM* pour *Electronic Document Management*) désigne un procédé informatisé visant à organiser et gérer des informations et des documents électroniques au sein d'une organisation. Le terme *GED* désigne également les logiciels permettant la gestion de ces contenus documentaires.

C. Gestion Electronique de Documents (GED) vs. Bigdata

490. La gestion électronique de documents (GED) a pour but de gérer des documents plus que des données ; elle sert également comme moteur à faciliter la recherche d'informations archivées sous forme électronique, à des fins de consultation partagée, de modification, d'enrichissement, de classement intelligent, surtout si les documents sont composites et multimédias : c.à.d. que le document contient à la fois un texte, graphique, son et/ou image animée ou fixe ; à la différence de l'EDI qui est un simple transfert par voie électronique, d'ordinateur à ordinateur, de données structurées, organisées en messages normalisés.

491. La GED est un concept produit suite à un besoin accru sur le marché d'avoir des outils pour maitriser et gérer les documents électroniques. Le concept GED peut être exécuté par l'adoption de différents genres de logiciel pour parvenir à cette fin.

492. Nous comparons la GED à une notion qui parait au premier abord similaire mais qui occupe une fonction plus vaste, et qui ne se limite pas à la seule gestion des documents électroniques. Cette notion est le « *bigdata* ».

493. *À force d'agrémenter le quotidien, ces nouvelles technologies finissent par s'immiscer dans la vie privée et même intime, parfois à notre insu, passant – pour reprendre l'expression de Madame le Professeur Laure Marino, des « little data aux big data » et, ce faisant, de « little brother » à « Big Brother »*[244].

[244] L. Marino, *Notre vie privée : des little data aux big data, Le secret dans la vie des personnes, in Le secret à l'ère de la transparence : JCP E 2012, suppl*. n° 47, p. 14. – V. également, L. Marino, *Le big data bouscule le droit : RLDI* déc. 2013, n° 3300. – V. également d'une manière générale sur le *big data*, Groupe de l'article 29, 16 sept. 2014, *WP 221*. – A. Bensamoun et C. Zolynski, *Big data et privacy : comment concilier nouveaux modèles d'affaires et droits des utilisateurs : LPA* 18 août 2014, n° 164, p. 8. – V. sur la réexploitation par le *Big Data* des données traitées dans le cadre du *quantified-self*, M. Lanna, Le quantified-self, nouveau moteur du *big data* et menace pour la vie privée : *LPA* 12 mai 2016, n° 95, p. 6. – V. pour une analyse du point de vue de la science politique, J. Boyadjian, La science politique face aux enjeux du « *big data* » et de la protection des données personnelles sur internet *: RD pub*. 2016, n° 1, p. 7. – V. pour une évolution au regard de la proposition de règlement, A. Latreille et C. Zolynski, in TEE, La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau Trans Europe Experts, ss la dir. de N. Martial-Braz : Société de législation comparée, 2014, p. 262.

494. La notion de *bigdata* est un concept s'étant popularisé en 2012 pour traduire le fait que les entreprises sont confrontées à des volumes de données (data) à traiter de plus en plus considérables et présentant un fort enjeu commercial et marketing[245].

495. D'ailleurs, ce concept de *bigdata* n'est pas propre au marketing, mais il est aussi important pour le développement du commerce électronique. D'après Evan Stubbs, *bigdata* est un "*terme familier qui se réfère à des ensembles de données qui sont trop lourds à traiter dans un laps de temps raisonnable en l'absence d'outils spécialisés. Les caractéristiques communes comprennent essentiellement de grandes quantités de données (volume), différents types de données (variété), et la vitesse sans cesse croissante de production (vitesse). Ils nécessitent généralement des mesures particulières pour la capture, le traitement, l'analyse, la recherche et la visualisation*"[246].

496. De cette définition, le *bigdata* est un terme qui signifie littéralement « grosses données », ou « méga-données », et parfois appelées données massives, et qui désigne l'ensemble de données qui deviennent tellement volumineuses qu'il en devient difficiles de travailler avec des outils classiques de gestion de base de données ou de gestion de l'information[247].

497. Le *bigdata* est conçu pour répondre à une problématique technique qui est la capacité de gérer d'énormes volumes de données en temps réel. Ainsi il y a 3 mots clé pour réaliser cet objectif qui sont le Volume, la Vitesse et la Variété.

– **Volume** car les masses de données à traiter sont sans cesse croissantes. Les secteurs concernés par le *bigdata* sont le plus souvent ceux qui par nature génèrent d'énormes volumes de données à traiter.

---

[245] B. Batelot, « *Définition : Big Data* », 1er septembre 2016, [En ligne : http://www.definitions-marketing.com/definition/big-data/].

[246] *Big Data* is defined as *"a colloquial term referring to datasets that are otherwise unwieldy to deal with in a reasonable amount of time in the absence of specialized tools. Common characteristics include large amounts of data (volume), different types of data (variety), and ever-increasing speed of generation (velocity). They typically require unique approaches for capture, processing, analysis, search, and visualization".* EVAN STUBBS, *Big Data Big Innovation – Enabling Competitve Differentiation through Business Analytics, edition John Wiley & Sons*, 2014, p.206.

[247] *Ibid.*

– **Vitesse** car la collecte, l'analyse et l'exploitation des données doit de plus en plus souvent se faire en temps réel, pour être efficace et répondre à leur fin.
– **Variété** car les données sont bien souvent de formes très variées et pas toujours structurées.

498. Aujourd'hui toutes les entreprises gèrent de la donnée (data), et leur compétitivité dépend à leur connaissance de la culture *data*. Car les entreprises ont certainement des marges de manœuvre assez importantes dans l'utilisation de leurs données. Nous nous interrogeons sur la façon dont une entreprise peut utiliser ses données, et quelles opportunités seront ouvertes dans leurs métiers. Il s'agit d'une vision de la capacité du système d'information à créer de la valeur. Le *bigdata* permet aux entreprises de mettre en valeur les données dont elles disposent et de trouver les informations qui leur permettent d'optimiser leur activité et rendre des services plus concrets à leurs clients.

III. La confiance dans le document électronique

499. Pour maintenir une bonne gestion des différents risques juridiques relevant de l'utilisation des documents électroniques, chaque partie doit d'abord être en mesure d'avoir une confiance raisonnable en l'identité numérique déclarée par une personne dans un document électronique.

500. Ces besoins d'authentification, notamment à l'occasion de signatures électroniques, existent tant au sein d'une entreprise ou d'un groupe, que dans les relations commerciales, qu'elles soient internes ou internationales.

501. Au fur et à mesure de l'évolution des technologies de l'information, des nouvelles méthodes ont été conçues afin de relier une donnée sous forme numérique à une personne définie ; ceci afin d'assurer l'intégrité de l'information ainsi que de permettre à cette personne de démontrer qu'elle a le droit ou l'autorisation d'accéder à un certain service ou à une certaine source d'information.

502. Sur le plan juridique, en cas de différend, les acteurs doivent pouvoir déterminer où se fier à l'identité numérique d'une personne afin d'être en position de lui imputer un acte ou un fait juridique. Ainsi l'identité d'une personne est essentielle pour pouvoir introduire une action en justice contre celle-ci, devant un tribunal territorialement compétent.

503. L'authentification est généralement précédée d'une identification ; cette dernière qui permet à une personne ou une entité de se faire reconnaitre du système au moyen d'un élément dont nous l'avons doté.

504. Le terme 's'identifier' consiste à communiquer une identité préalablement enregistrée, alors que 's'authentifier' consiste à apporter la preuve de cette identité. Bien que nous traitions l'identification en plus de détail dans la deuxième partie du plan sous l'angle de l'identification du porteur du document électronique, il nous convient de soulever quelques points importants nous aidant à distinguer l'authentification de l'identification.

A. Identification des documents électroniques

505. L'identité sous forme numérique se pose aujourd'hui de façon urgente avec le développement fulgurant des espaces de communication et d'expression sur l'Internet. Il s'agit d'une notion encore complexe que les travaux en sciences humaines et sociales tentent de cerner d'après le rapport Truche[248] :

'*Le concept même d'identité numérique n'est pas, et pas plus que l'identité traditionnelle univoque et uniforme : l'identité numérique se compose d'un ensemble d'identifiants partiels, finalisés, et des relations qu'entretiennent ces identifiants.*

[248] Pierre Truche, Jean-Paul Faugère, Patrice Flichy, *Administration électronique et protection des données personnelles – Livre Blanc*, http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000100/0000.pdf, consulté le 26 mars 2016.

506. Généralement, l'identification se définit comme *une opération permettant à un individu de faire état de son origine sur la base d'un élément externe, d'exprimer son identité*[249].

507. Dans ce sens, l'identification peut se caractériser à travers tout document pouvant attester de l'origine d'une personne ; ce pourrait être par exemple un extrait de naissance, une carte d'identité ou même un permis de conduire. L'identification peut aussi se réaliser sur la base d'un élément externe tel que le témoignage de tiers.

508. Ainsi, le terme 's'identifier' signifie le fait de communiquer une identité, préalablement enregistrée de la personne, qui a un caractère permanent et inhérent à la personne; alors que le terme 's'authentifier' relève de la vérification de l'exactitude de cette identité, en apportant la preuve.

509. Dans le contexte numérique, l'identification des personnes constitue la condition *sine qua non*[250] de la sécurité des échanges sur les réseaux numériques, qu'il s'agisse de transactions commerciales ou administratives ou de simples correspondances privées. Sur ce point, ce qui pourra soulever un défi dans la société d'information aujourd'hui c'est le droit à l'anonymat.

510. D'un point de vue littéral, le mot 'anonymat' signifie un faux nom qui est choisi par une personne. Toutefois, l'anonymat ne doit pas avoir pour objectif d'interdire que nous retrouvions l'identité des personnes en cas de nécessité, tout spécialement en cas d'infraction et de poursuites judiciaires.

511. En France, par exemple, en vertu de l'article 6-II de la LCEN[251], les fournisseurs d'accès et les hébergeurs de contenus sont soumis à une obligation de détenir et de conserver les données de nature à permettre l'identification des

[249] Eric A Caprioli, *Signature électronique et dématérialisation, Edition LexisNexis SA* 2015, p. 28 s.
[250] *Sine qua non* est un terme juridique latin qui signifie une condition nécessaire « sans laquelle cela ne pourrait pas être ».
[251] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. [En ligne : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=id].

personnes qui ont contribué à la création du contenu ou l'un des contenus des services dont elles sont prestataires.

512. Cependant, ces identifications ne touchent que les contenus diffusés sur Internet et non pas les transactions ou les accès en ligne à des données ou à des services. En droit européen, nous saisissons une définition de l'identification électronique prévu à l'article 3 (1) de la proposition de règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur[252].

513. Ce texte l'a défini comme le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière claire et non équivoque une personne physique ou morale.

514. D'ailleurs, la proposition de règlement de l'Union européen n° 910/2014 a initié une définition de l'expression 'moyen d'identification électronique', comme celui ayant pour objectif de permettre l'accès à des services en ligne, peu importe que ce moyen soit matériel (*token*, à savoir un boitier électronique qui génère des jetons d'authentification) ou immatériel (art. 3-2[253]).

515. La proposition de règlement a aussi défini le 'schéma d'identification électronique', en tant que système permettant l'identification électronique en vertu duquel de moyens d'identification électronique sont délivrés à des personnes physiques ou morales[254].

516. Pourtant, dans le numérique, l'identification est souvent associée à l'authentification dans sa fonction de vérification de l'identité déclarée par le biais de l'identification électronique.

[252] Article 3 (1) du Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, [En ligne : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32014R0910].
[253] Article 3 (2) du Règlement (UE) n ° 910/2014, *ibid.*
[254] Article 3 (4) du Règlement (UE) n ° 910/2014, *ibid.*

B. Authentification des documents électroniques

1) Contexte et notion.

517. Le besoin accru de la garantie de sécurité dans les communications électroniques en matière d'identification des personnes a entamé les discussions vers le recours à l'authentification pour prendre ainsi le relais sur physique traditionnelle avec, pour finalité, de vérifier l'identité dont une personne se réclame[255].

518. En Europe, les pays suivent la tradition civiliste, et le concept d'authentification est interprété de façon assez étroite. Par exemple en droit civil français, l'authentification consiste en l'opération destinée à conférer à un acte, le caractère authentique.

519. Le terme 'authentique'[256] signifie que le document est vérifié et certifié par une autorité publique compétente (soit une juridiction ou un état civil) ou par un officier public et ministériel dont les pouvoirs ont été délégués par une autorité publique (comme les notaires et les huissiers de justice).

520. En procédure civile, c'est bien souvent le cas de se référer à la notion de document authentique et original. Dans le même raisonnement, le caractère authentique d'un document renvoie à sa nature sincère, c.-à-d. qu'il émane bien des signataires, et qu'il constitue l'*instrumentum* original des informations qu'il contient, sans altération ni modification depuis son établissement[257].

521. Pendant longtemps, il n'existait pas une définition juridique précise de l'authentification au niveau européen ; pour suppléer à cette carence législative, il a fallu renvoyer aux dispositions relatives à la signature électronique en tant que méthode efficace d'authentification.

---

[255] Eric A Caprioli, *Op. cit.*, p. 30 s.
[256] *Lexique des termes juridiques*, *Dalloz*, 18° éd. 2014, p.81, V° *Authentification*. L'acte authentique est une « attestation de l'exacte provenance d'un objet ou d'un écrit ».
[257] E. A. Caprioli, *la sincérité de la signature électronique*, *in* O. Le Bot (sous la coordination), *la sincérité en droit*, Bruxelles, Larcier, 2011, p. 111-127, [En ligne: http://www.caprioli-avocats.com/publications/54-dematerialisation-archivage/246-la-sincerite-de-la-signature-electronique].

522. Ainsi, l'article 3 (10) du règlement de l'Union européen n° 910/2014[258], définit la signature électronique comme "*des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer*".

523. D'ailleurs, la première véritable définition juridique de l'authentification a été introduite dans le règlement communautaire n° 460/2004 du 10 mars 2004[259] instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA).

524. Selon son article 4-e, l'authentification doit être entendue comme *la confirmation de l'identité prétendue d'entités ou d'utilisateurs*. Cette définition porte un sens assez large puisqu'elle intègre les personnes morales. Celle-ci a été reprise en droit français par le Référentiel général de sécurité (RGS) [260], ce cadre réglementaire ayant pour objectif principal l'instauration et le renforcement de la confiance des usagers dans les services électroniques mis à disposition par les autorités administratives.

525. Ce référentiel général de sécurité est pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives.

526. Dans le cadre du développement des téléservices et des échanges électroniques entre l'administration et les usagers, les autorités administratives

---

[258] Article 3 (10) du Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, [En ligne : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32014R0910].

[259] Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (Texte présentant de l'intérêt pour l'EEE), [En ligne: http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32004R0460].

[260] Le référentiel général de sécurité (RGS) est le cadre règlementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens. Le site gouvernemental de l'RGS dans le lien suivant : http://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/.
[En ligne : http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf].

doivent garantir la sécurité de leurs systèmes d'information en charge de la mise en œuvre de ces services.

527. Ainsi la définition de l'authentification a été reprise dans le paragraphe 3.2 du RGS en prévoyant que '*l'authentification a pour but de vérifier l'identité dont se réclame une personne ou une machine*'.

528. Depuis l'entrée en vigueur du règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, nous disposons de l'article 3 qui prévoit une définition à l'authentification: *'un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique'*.

529. Si cette définition reprend l'idée de vérification ou de validation de l'identification électronique, elle étend le concept d'authentification à la validation de l'origine et de l'intégrité d'une donnée électronique.

530. Dans le contexte international, ni la loi-type de la CNUDCI sur le commerce électronique, ni la loi-type de la CNUDCI sur les signatures électroniques n'emploient le terme 'authentification' dans divers systèmes juridiques et de la confusion possible avec des procédures ou des exigences de formes particulières. Par ailleurs, s'il fait état de l'authentification dans le Guide d'incorporation de la loi-type de la CNUDCI sur le commerce électronique, elle n'a trait qu'à l'authentification des messages ou des données.

2) Les procédés d'authentification

531. Nous disposons de deux méthodes d'authentification pour vérifier l'identité de la personne ou l'entité à l'origine de l'acte.

- ***Authentification simple :***

532. L'authentification est un mécanisme qui ne requiert qu'un seul facteur, le plus souvent un mot de passe et/ou un identifiant[261].

533. C'est ici l'authentification dans sa forme simple lorsque le moyen permettant d'effectuer l'identification dépend d'un seul domaine : celui-ci peut être soit un facteur matériel (ce que l'utilisateur possède, par exemple, une clé USB, un *token* ou une carte à puce), soit un facteur inhérent à la personne comme la biométrie (ce que l'utilisateur expose de sa personne, par exemple, une empreinte digitale ou une empreinte vocale).

534. Il est évident qu'une identification qui passe par un seul canal se trouve plus vulnérable aux attaques des hackers qu'un dispositif s'appuyant sur au moins deux facteurs d'authentification, ce que nous allons envisager comme deuxième méthode d'identification détenant un système de sécurité renforcée.

- ***Authentification forte :***

535. Les méthodes d'authentification fortes sont plus fiables que les simples et elles permettent de prévenir plus efficacement (notamment en cas d'échanges de données sensibles) les usurpations d'identité, les accès sans droit, les fraudes commises en ligne sur les comptes bancaires, etc.[262].

536. Elles imposent une combinaison de deux canaux distincts et de deux facteurs : par exemple, un login (identifiant)/mot de passe saisi en ligne et un autre code généré de façon aléatoire (OP non rejouable), utilisable pendant une courte période de temps et envoyé via le téléphone mobile (SMS) ou un *token*.

537. D'ailleurs, à partir du moment où nous acceptons qu'un pré-requis de l'instauration d'un régime de confiance sur les réseaux consiste en la possibilité d'imputer toute action ou opération à une personne déterminée, nous saisissons bien l'importance de cette phase d'authentification pour tout service de l'Internet, et notamment pour les services bancaires et de paiement en ligne.

[261] Eric A Caprioli, *Signature électronique et dématérialisation, Edition LexisNexis SA* 2015, p. 36.
[262] Eric A Caprioli, Op., cit., p. 36 s.

538. Ainsi par exemple la communauté bancaire a mis en œuvre certaines initiatives en ce sens, comme la publication d'une Politique d'acceptation commune (PAC) des certificats par le Comité français d'organisation et de normalisation bancaire. Cette initiative a pour objectif de permettre la reconnaissance des certificats d'identification électronique de clients entre établissements bancaires et financier l'ayant acceptée.

IV. LES RÈGLES DE LA PREUVE ET LA PRÉSOMPTION DE FIABILITÉ DE LA SIGNATURE ÉLECTRONIQUE

A. Notion de la preuve.

539. La preuve est une notion dominante, car c'est grâce à la preuve que le juge peut reconnaitre le droit du justiciable et parvenir à un verdict pertinent qui obéit à sa conscience en tant que serviteur de la justice, et de la règle de droit.

540. Pourtant, la notion de la preuve n'est pas légalement définie, et la loi se contente d'énumérer les moyens dont nous pouvons l'administrer. Même si le terme apparait d'une clarté évidente, son étude fut l'objet de nombreuses interprétations doctrinales et des prolongements philosophiques et moraux dépassant les préoccupations juridiques.

541. Afin de suppléer à cette carence et le silence de droit à son sujet, la doctrine a proposé une définition ayant une approche philosophique pour reconnaitre la notion de 'la preuve'. Ainsi Domat écrivait « *c'est tout ce qui persuade l'esprit d'une vérité* ». La preuve *permet à celui qui se prévaut d'une affirmation de la faire reconnaitre comme vraie et d'en tirer toutes les conséquences juridiques qui y sont attachées*[263].

[263] Rapport de l'Assemblée Nationale au nom de la commission des lois constitutionnelles, de la législation et de l'administration générales de la république sur le projet de loi, adopté par le Senat, portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique, M. Christian PAUL. 28 fév. 2000.

542. D'ailleurs, il nous faut citer ici un vieil adage du droit : *idem est non esse et non probari*[264] (ne pas être ou ne pas être prouvé, c'est tout un/ avoir un droit sans le prouver revient à ne pas avoir le droit). Cette tradition juridique retenue du droit romain nous enseigne que pour que le juge tienne compte d'un fait, il faut le prouver. S'il n'est pas prouvé, le fait n'existe pas pour le juge.

543. Pour se prononcer dans un litige, le juge confronte les éléments de fait avec les éléments de droit et il base sa décision sur les règles de la preuve. Ainsi, la preuve présente le seul moyen employé pour convaincre le juge et parvenir à un verdict favorable. Il s'agit d'un élément essentiel de l'application du droit.

« La preuve juridique est une preuve judiciaire ».

B. Régimes de la preuve.

544. Nous estimons que la preuve est une constante du droit. Elle existe dans tous les droits, même pour les plus « primitifs ». La preuve est une notion juridique essentielle dans tous les systèmes juridiques et toute prétention juridique doit être justifiée par la preuve des droits invoqués.

545. La preuve repose sur la nécessité de convaincre un juge ou un arbitre sur la base d'éléments pertinents qui lui permettent de déduire les conséquences juridiques posées par une règle de droit. Avec les technologies de l'information et de la communication (TLC), de nouvelles règles de preuve ont été posées pour les actes juridiques comme les contrats et les documents électroniques.

546. À la fin du XXe siècle, en raison de l'utilisation accrue de l'informatique au sein des entreprises, la problématique s'agissant de l'écrit papier par rapport à l'écrit électronique se posait : quel document prévalait juridiquement sur l'autre ? L'écrit papier était-il plus probant ? Comment faire valoir juridiquement l'écrit électronique ?

---

[264] Philippe OBADIA, *« Idem est non esse aut non probari = avoir un droit sans le prouver revient à ne pas avoir de droit »*, [En ligne : https://www.fidealis.com/fr/actualites-35-Idem+est+non+esse+aut+non+probari+%3D+avoir+un+droit+sans+le+prouver+revient+%C3%A0+ne+pas+avoir+de+droit.html].

547. En principe, il existe deux grands systèmes de preuve: le *système de preuve libre* et le *système de preuve légale*[265]. Le premier vise la capacité pour les parties de présenter toute forme de moyens de preuve à l'appui de leur demande. Un tel système laisse au juge le soin d'admettre, au cas par cas, si les moyens de preuve qui lui sont présentés sont recevables. Une question laissée à la libre appréciation des juges.

548. Dans le second régime, la loi impose aux parties certains moyens de preuve et guide ainsi l'intervention du juge qui est chargée de contrôler la conformité des preuves exigées par la loi et ne dispose d'aucun pouvoir pour en apprécier la portée.

549. En droit français, le système probatoire est mixte, les deux systèmes s'appliquent respectivement selon les différentes branches du droit, voire les deux peuvent coexister dans certaines branches.

550. Ces deux systèmes présentent un enjeu important ; lorsque le système probatoire est libre, le juge n'a pas à s'interroger sur la question de savoir si l'écrit versé comme pièce au débat constitue ou non une preuve admissible et emporte un haut degré de crédibilité.

551. Ainsi, les preuves résultant de l'emploi des nouvelles technologies seront librement admissibles devant le juge pénal, quel que soit le support électronique qui les soutient. Bien entendu, le juge ne peut pas se servir de preuves qui ont été estoquées comme les écoutes téléphoniques, mais il pourra ordonner des expertises afin de vérifier la véracité du moyen utilisé comme preuve et venir conforter et asseoir sa conviction.

552. En matière pénale, l'article 427 du Code de procédure pénale dispose que « *Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction.*

[265] Sur ce point, voir : CAPRIOLI (E.), *Op. cit.*, n°801 s.

Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui ».

553. Le régime de la preuve est donc principalement dominé par deux principes fondamentaux : *la liberté de la preuve et son corollaire, l'intime conviction du juge*[266]. La liberté de la preuve signifie que tout moyen de preuve est admissible et qu'il n'existe pas de hiérarchie des preuves. Bien que la preuve soit libre, cela ne signifie que le système est affranchi de toute règle. La preuve devra toujours être apportée dans des conditions loyales et soumise à la contradiction[267]. Le principe de l'intime conviction obéit en effet à la règle du jeu de l'alinéa 2 de l'article 427 du Code de procédure pénale ; la preuve doit pouvoir être débattue par les parties.

554. De la même manière, le juge administratif ne connaitra pas les problèmes qui peuvent naître de l'apparition de nouveaux procédés scientifiques ou techniques de constatation de la vérité. En matière commerciale, le juge pourra même retenir à titre de présomption simple la composition d'un code confidentiel d'un system informatique fonctionnant régulièrement[268].

555. En revanche, lorsque le système probatoire est réglementé, le juge devra rechercher si la pièce qui lui est soumise relève du mode de preuve légalement admis par le texte en cause. Dans l'affirmative, le juge devra alors s'incliner et ne pourra accorder une portée moindre au moyen de preuve rapporté.

556. D'après le droit français, l'article 1315-1 du Code civil dispose de cinq différents moyens de preuve : la preuve littérale, la preuve testimoniale, les présomptions, l'aveu de la partie et le serment.

557. Etant donné que l'écrit est au cœur de notre étude, le juge devra déterminer si les écrits que les parties produisent relèvent de la qualification de la preuve littérale ou non. Dans l'affirmative, il sera alors lié par leur force probante.

---

[266] CAPRIOLI (E.), *Op. cit.*, n°802 s.
[267] *Ibid*
[268] Hervé de GAUDEMAR, « *La preuve devant le juge administrative* », *Droit Administratif* n° 6, Juin 2009, étude 12, LexisNexis, n°10 s.

558. Sur la preuve légale, en droit français, le texte de l'article 1341 du Code civil est d'une portée générale. En citant ce texte considéré comme pièce fondamentale du système de preuve légale : « *il doit être passé acte devant notaires ou sous signatures privées de toute chose excédant une somme ou une valeur fixée par décret, même pour dépôts volontaires, et il n'est reçu aucune preuve par témoins contre et outre le contenu aux actes, ni sur ce qui serait allégué avoir été dit avant, lors ou depuis les actes, encore qu'il s'agisse d'une somme ou valeur moindre. Le tout sans préjudice de ce qui est prescrit dans les lois relatives au commerce* ».

559. Cet article a fait référence au décret d'application modifiant la procédure civile du 20 aout 2004, et qui prévoit que la preuve des actes juridiques peut être apportée par tout moyen jusqu'à 1,500 euros et qu'au-delà, une preuve littérale est nécessaire, à défaut, il ne s'agirait que d'un commencement de preuve par écrit. Aussi nous retenons du texte de l'article 1341 du Code civil la règle de droit suivante:

560. Par rapport à l'écrit électronique entre un acte authentique et un acte sous seing privé, il s'agit de l'obligation de pré-constituer un écrit sous la forme d'un acte authentique ou d'un acte sous seing privé pour des opérations juridiques supérieures à un certain seuil. Pour employer les termes exacts, l'écrit papier est un acte juridique sous seing privé sur support papier et l'écrit électronique, un acte juridique sous seing privé sous forme électronique.

561. Le législateur français a consacré explicitement le principe de la neutralité du support de l'acte juridique ; au terme de l'article 1316-1 du Code civil: *"l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier (...)*".

562. Il faut ici rappeler que la définition de l'article 1316 du Code civil propose simplement une définition de l'écrit, indépendamment de son support et de son mode de transmission. L'article 1316 du Code civil ne permet donc pas de déterminer ce qui constitue une preuve littérale opératoire. (*Supra*).

563. De plus, le même principe de neutralité a été mentionné implicitement dans le texte de l'article 1326 du Code civil[269] ; en fait, le législateur français a modifié ce dernier par la loi n° 2000-230 du 13 mars 2000, dans son article 5[270] dans le sens où il a supprimé la référence à l'écrit manuscrit, afin de reconnaitre implicitement l'écrit électronique en tant que preuve légale en droit français.

564. Une autre distinction apparait dans la doctrine entre les exigence *ad probationem* et *ad validitem*, lorsque nous opposons deux grands courants, consensualisme et formalisme. La règle générale de droit édicte que les actes juridiques, tels que les contrats, se forment par le seul échange des consentements, ce qui suppose que la rédaction et la signature d'un écrit ne soient pas nécessaires à leur formation.

565. Les actes juridiques doivent toutefois répondre à certaines conditions de fond (i.e. consentement, capacité, objet et cause) et, par exception, à des conditions de forme. Pour ces dernières nous parlons de formalisme juridique[271].

566. Ainsi, nous présentons un contrat comme solennel lorsqu'en plus de l'échange de consentements, une formalité supplémentaire est accomplie et nécessaire. Les exigences d'un écrit peuvent être fixées de deux manières par le droit positif : sur le plan de la preuve (*'ad probationem'*) et sur celui de la validité (*'ad validitatem'*). Les conséquences de leur absence sont par principe différente : « s'il l'est seulement pour servir de moyen de preuve *ad probationem*, son absence n'affecte pas la validité de l'opération ; s'il l'est comme condition de validité de l'acte juridique *'ad validitatem'*, l'acte juridique passé sans écrit est nul.

---

[269] Article 1326 du Code civil français (Modifié par Loi n°2000-230 du 13 mars 2000 - art. 1 JORF 14 mars 2000) prévoit que "*l'acte juridique par lequel une seule partie s'engage envers une autre à lui payer une somme d'argent ou à lui livrer un bien fongible doit être constaté dans un titre qui comporte la signature de celui qui souscrit cet engagement ainsi que la mention, écrite par lui-même, de la somme ou de la quantité en toutes lettres et en chiffres. En cas de différence, l'acte sous seing privé vaut pour la somme écrite en toutes lettres*".

[270] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, version consolidée au 31 octobre 2016, [En ligne : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629200].

[271] CAPRIOLI (E), *Op. cit.*, note n°86 et s.

567. En ce qui concerne les exigences à des fins de validité des actes juridiques (par ex., les contrats qui imposent l'exigence d'un écrit comme les contrats de bail, de crédit à consommation, de vente par démarchage a domicile, les statuts de société, la cession et la licence de brevet d'invention, etc.), la loi n 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) a introduit, dans le Code civil, les article 1108-1 et 1108-2[272] relatifs à la validité des actes juridiques conclus sous forme électronique.

C. La valeur juridique de la signature numérique

568. Considérée comme l'un des instruments garantissant l'identification et l'intégrité des documents électronique, la signature numérique de la norme ISO[273], un système de traitement de l'information crée en 1989 donne la première définition de la signature numérique comme "*données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de donnée et protégeant contre la contrefaçon*".

569. L'instrument de la signature numérique apporte le standard l'identification et l'intégrité. C'est pourquoi, cet outil sécuritaire a bénéficié d'une reconnaissance juridique par la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques[274], transposée dans le droit interne de chaque État membre sous le nom de signature électronique.

[272] Voir *supra* n°14.
[273] ISO 7498-2 est un système de traitement de l'information produit en 1989, il fournit une description générale des services de sécurité et des mécanismes connexes, qui peut être assurée par le modèle de référence, et des positions au sein du modèle de référence où les services et les mécanismes peuvent être fournis. Il étend le champ d'application de la norme ISO 7498 pour couvrir des communications sécurisées entre les Systèmes Ouverts. ISO 7498-2 ajoute aux concepts et aux principes énoncés dans la norme ISO 7498 mais ne les modifie pas. Il ne contient pas pour autant de spécification de mise en œuvre, ni une base pour évaluer la conformité des mises en œuvre en vigueur.
[274] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, Journal Officiel des communautés européennes 19 Janvier 2000. [En ligne : http://data.europa.eu/eli/dir/1999/93/oj].

570. D'une part, la directive du 13 décembre 1999 sur la signature électronique pose un principe de non-discrimination entre les actes constatés sur support papier et ceux constatés sur support numérique.

571. L'article 1316-1 du Code civil affirme le principe d'équivalence entre l'écrit sur support papier et l'écrit sur support électronique. Il définit « l'écrit électronique parfait » : la personne dont il émane doit être dûment identifiée et il doit être établi et conservé de manière à préserver son intégrité. En réalité, ces deux conditions (« personne dûment identifiée » et « intégrité de l'acte ») font référence à l'article 1316-4 al 2 du Code civil qui définit la signature électronique qui « consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle se rattache ».

572. Nous nous demanderons s'il n'est pas redondant dans l'article 1316-1 du Code civil d'indiquer une condition d'identification alors que celle-ci a déjà été consacrée à l'article 1316-4 du Code civil. Si tel n'était pas le cas, cela signifierait qu'un écrit dont nous savons de qui il émane sans qu'il soit pour autant signé – sous réserve qu'il remplisse la seconde condition d'intégrité – est une preuve littérale.

573. En conséquence, l'expression « identification de la personne dont l'écrit émane » doit être maniée avec précision et vigilance. Il s'agit de bien comprendre ce que signifie le terme « émaner » pour prendre toute la mesure de l'exigence.

574. Concernant la signification du verbe "émaner", nous employons ce terme pour désigner qu'il est l'œuvre personnelle de son auteur. Ce terme "émaner" provient du latin "*emanare"* qui signifie "provenir de, sortir de, découler de". Dès lors, exiger de l'écrit sous forme électronique qu'il émane de son auteur ne consiste pas seulement à imposer qu'il soit le produit personnel de celui-ci, mais suppose également que l'écrit, en lui-même, singularise l'auteur. Par définition, le terme 'émaner' implique toujours une fusion entre le sujet et l'objet issu de l'acte produit par le sujet, en tant qu'émanation d'un individu.

575. Cependant, en cas d'incertitude sur l'intégrité ou l'authenticité entre deux preuves inscrites sur deux supports différents - papier et électronique -, le législateur confie au juge la tâche de désigner la preuve la plus convaincante aux faits de l'espèce. Dans ce sens, l'article 1316-2 du Code civil dispose que : « *Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support* ».

576. En pratique, si l'authenticité ou l'intégrité d'un document sont contestées, un expert peut être interpellé pour décider du caractère probant dudit document. En dernier lieu, le juge forgera sa décision en fonction du niveau de protection que l'entreprise aura mis en place dans le but de garantir la force probante des données, et en fonction de l'expertise. Cette dualité de nature technique et juridique explique qu'il est possible dans certaines applications ou services de trouver soit une signature à finalité purement technique, soit une signature à finalité juridique, soit les deux[275].

577. Par ailleurs, de multiples questions sur la signature électronique avait fait l'objet des nombreux débats et qui en avait abouti à la publication de la Loi type de la CNUDCI sur les signatures électroniques[276].

578. La Convention des Nations Unies sur l'utilisation des communications électroniques dans les contrats internationaux se base principalement sur deux groupes d'éléments identifiés à l'article 9 (3). Elle concerne les deux fonctions cumulatives de la signature, conformément au principe de l'équivalence fonctionnelle (un principe que nous discuterons en détail dans la deuxième partie de la présente recherche), à savoir, l'identité du signataire et l'intention liée à « l'information contenue dans la communication électronique ». Le second évoque de surcroît un certain niveau de fiabilité, proportionnel aux circonstances.

[275] V. A. 27 juin 2007 portant application de l'article *D.* 1617-23 du Code général des collectivités territoriales relatif à la dématérialisation des opérations en comptabilité publique *: Journal Officiel* 11 Juillet 2007.

[276] La loi-type de la CNUDCI sur les signatures électroniques, en date de 5 juillet 2001, *Publication des Nations Unies, New York,* 2002.

579. Par analogie, et en application du principe du "parallélisme des formes", comme nous exigeons que le document papier porte une signature manuscrite, nous approuvons l'usage de la signature électronique pour le document électronique.

580. En effet la signature électronique présente ici au niveau technique un grand avantage par rapport à l'écrit sous forme manuscrite : ce qu'elle permettrait l'identification du signataire et l'intégrité du document signé. Et c'est précisément cela que nous attendions de l'écrit électronique.

581. En France, la réforme du droit de la preuve consacre l'écrit et la signature électroniques (*L. n° 2000-230, 13 mars 2000* portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

582. La loi du 13 mars 2000 a mis sur pied d'égalité la signature électronique et la signature manuscrite, à trois conditions pour la première :

- il faut une procédure d'identification ;
- il faut qu'il existe un lien entre le contenu du document numérique et son destinataire ;
- le document doit être conservé de manière intègre ;

583. D'ailleurs, ayant pour objectif d'encourager le recours à la signature électronique, le législateur a créé une présomption de fiabilité de la signature électronique ; ce qui implique que la charge de la preuve incombe alors à l'autre partie.

584. C'est le texte de l'article 2 du décret du 30 mars 2001 qui prévoit la présomption de fiabilité du procédé de signature électronique lorsque « *ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié* ». Nous retenons de ce texte trois exigences à remplir pour pouvoir reconnaitre une signature électronique:

- il faut utiliser un dispositif de création sécurisé de la signature ;

- il faut la délivrance d'un certificat qualifié ; cette condition implique que le prestataire de services de certification soit lui-même qualifié.
- la signature doit être sous le contrôle exclusif du signataire.

585. Par conséquent, l'écrit numérique a la même valeur probatoire que l'écrit papier. Pourtant les conditions pour en faire un mode de preuve ne sont pas toujours évidentes à remplir, une raison pour laquelle la signature est sécurisée par des mécanismes modernes de cryptologie.

PARAGRAPHE II : MÉCANISMES DE LA CRYPTOLOGIE

586. La cryptologie est un outil essentiel pour maintenir la signature électronique à l'abri de toute manœuvre frauduleuse de falsification du document électronique. Nous étudierons ici les mécanismes de la cryptologie et le chiffrement du document électronique (I).

587. Par la suite, nous évoquons les nouveaux mécanismes et services informatiques de sécurité des données électroniques, dont la notion de « *Cloud computing* » ou bien en français « l'informatique en nuage » (II).

I. Mécanisme de la cryptologie à clé publique - Cryptographie de la signature électronique

A. Contexte des services de cryptologie

588. La signature électronique de l'*article 1316-4* du Code civil[277] fait appel à des mesures cryptographiques. A l'origine, étant une pratique réservée aux

[277] Article 1316-4 du Code civil : « *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat* », [En ligne : https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006437841&cidTexte=LEGITEXT000006070721].

militaires, policiers et diplomates[278], la cryptologie était jusqu'aux années 1990 considérée comme une arme de guerre (*L. n° 90-1170, 29 déc. 1990, art. L. 28, 2°)* avant la survenance de la dérégulation des télécommunications qui a trouvé son apothéose avec la loi n° 2004-575 du 21 juin 2004 relative à la confiance dans l'économie numérique.

589. Le chiffrement a pour objectif principal d'assurer la confidentialité des informations transmises. L'usage des codes secrets est très courant dans l'histoire. Elle s'appuyait au début sur des formes primaires de steganographie[279] comme l'ont rapporté *Hérodote* ou *Jules César* dans la Guerre des Gaules jusqu'aux formes évoluées utilisées de nos jours[280].

590. Actuellement, la pratique utilise essentiellement les algorithmes mathématiques pour assurer la confidentialité des informations que nous entendons garder secrètes. Certains estiment même que la Seconde Guerre mondiale a été gagnée grâce au décryptage des informations transmises par les sous-marins allemands au moyen de la machine de chiffrement baptisé « *Enigma* »[281].

591. De nos jours, dans toutes les missions diplomatiques, il y a une salle du chiffre, à partir de laquelle sont envoyés les messages confidentiels vers la capitale. D'ailleurs, la valise diplomatique était utilisée à l'origine comme moyen de transport et de transmission des codes secrets. Il est clair que la cryptographie s'est développée dans le cadre militaire et de l'espionnage.

---

[278] Jean-Louis Autin et Pascale Idoux, *Fasc. 4600 : Droit National des Communications électroniques, 15 Janvier 2011*, mise à jour : 6 Février 2015 *JCP*, note n°129.

[279] Steganographie est un terme grec qui signifie l'ensemble de techniques permettant de transmettre une information en la dissimulant au sein d'une autre information (photo, vidéo, texte, etc.) sans rapport avec la première et le plus souvent anodine, essentiellement à l'aide de logiciels spécialisés. [En ligne :http://www.larousse.fr/dictionnaires/francais/st%C3%A9ganographie/10910018].

[280] S.Singh, Histoire des codes secrets, J.-C. Lattes, 1999. Hérodote disait que la méthode grecque consistait à écrire un message sur le crane rasé d'un messager, attendre que les cheveux aient repoussé, et l'envoyer à travers les positions ennemies jusqu'aux destinataires. Jules César dans la Guerre des Gaules utilisait la substitution de lettres avec une clé de répartition, ce qui rendait les messages interceptés incompréhensibles des Gaulois.

[281] "*Enigma*" est une machine électromécanique portable servant au chiffrement et au déchiffrement de l'information. Elle fut inventée par l'Allemand Arthur Scherbius, reprenant un brevet du Néerlandais Hugo Koch, datant de 1919. "*Enigma*" fut utilisée principalement par les Allemands *(Die Chiffriermaschine Enigma)* pendant la Seconde Guerre mondiale. http://www.bbc.co.uk/history/topics/enigma .

592. Ainsi, des multiples solutions techniques existent depuis longtemps et permettent d'offrir des garanties d'authentification de l'origine des informations, d'intégrité (pour s'assurer que la donnée n'a pas été altérée accidentellement ou frauduleusement), et de confidentialité des messages.

593. La technique de la signature électronique met en œuvre un procédé cryptographique pour pouvoir garantir l'intégrité du document signé et l'identité du signataire. Ce procédé de cryptographie est une technique qui sert à chiffrer un message, de le rendre inintelligible aux yeux de ceux qui ne sont pas les destinataires du message.

594. Avec des clés symétriques, il est possible de diffuser une clé permettant de déchiffrer les messages chiffrés avec la même clé restée secrète mais le problème réside dans la transmission de cette clé qui ne peut transiter sur les réseaux au risque d'être interceptée.

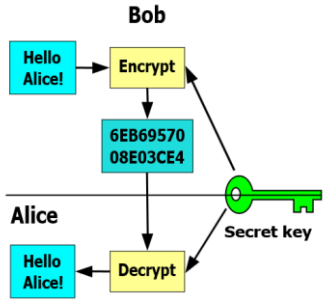

Schéma représente la cryptographie à clé symétrique (cryptographie à clef secrète), où une seule clé est utilisée pour le chiffrement et le déchiffrement

595. Pour résoudre ce problème, il est aujourd'hui recommandé d'utiliser des clés asymétriques en diffusant une clé publique pour permettre à des tiers de chiffrer les messages qu'ils souhaitent adresser à celui et lui seul qui conserve secrète la clé privée permettant de les déchiffrer[282].

[282] CAPRIOLI (E.), *Op. cit.*, page 215 s.

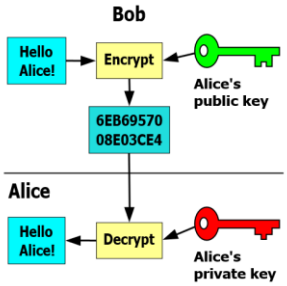

Schéma sur la cryptographie à clé publique, où des clés asymétriques sont utilisées pour le chiffrement et le déchiffrement

596. La signature électronique utilise la méthode de la cryptographie asymétrique. Celle-ci signifie que nous allons d'abord chiffrer le document que nous souhaitons envoyer à l'aide d'une clé (c.-à-d. de rendre le document inintelligible) et pour déchiffrer (voir rendre à nouveau le message intelligible), le destinataire devra utiliser une autre clé ; ainsi ceux que l'une peut faire, seule l'autre peut le défaire.

597. En fait, ces deux clés sont délivrées par un organisme tiers de confiance, appelé le prestataire de services de Certification Électronique (PSCE). Ces deux clés sont différentes, et désignées sous le terme de clé privée et de clé publique.

598. D'un côté, la clé privée qui est une clé personnelle utilisée uniquement pour le procédé de chiffrement ; de l'autre côté, la clé publique, remise par l'organisme de tiers de confiance à tous ceux dont nous voulons faire lire le document, servira donc au déchiffrement du message.

599. Donc, en cryptographie, nous utilisons des clés symétriques (uniquement pour le chiffrement) ainsi que des clés dites asymétriques (une clé privée qui reste secrète et une clé publique figurant dans un certificat) utilisées pour l'authentification, la signature électronique et le chiffrement.

600. Parlons de la technique de la cryptographie, le procédé de chiffrement s'effectue d'abord par l'extraction d'une partie du message que nous souhaitons

envoyer, grâce à la fonction mathématique dite de *hachage*[283]. Ce hachage est transmis avec le message que nous souhaitons envoyer, et il servira à vérifier que le message n'a pas été altéré puisque nous comparerons ce cours extrait 'haché' au message pour vérifier qu'ils sont identiques[284]. Ainsi la fonction de hachage permet essentiellement de garantir l'intégrité du message que nous désirons envoyer.

601. D'ailleurs, il faut s'assurer que le hachage n'a lui-même pas été altéré au cours de la transmission. C'est ainsi que cet extrait est chiffré également avec la clé privée de l'émetteur puis le destinataire le déchiffrera avec la clé publique.

602. Le message est ensuite envoyé avec le hachage au destinataire. Le message a lui été chiffré avec la clé publique du destinataire lequel pourra la déchiffrer seulement avec sa clé.

603. L'authentification du message[285] est ainsi possible grâce a ce mécanisme de cryptologie et d'hachage, puisque si le message est déchiffré avec la clé diffusée, le message a été chiffré avec la clé demeurée secrète (la clé privée) et donc cela prouve que le message émane bien de celui qui la détient. L'origine du message est ainsi vérifiée. De plus, si cette vérification s'effectue au moyen d'un certificat électronique d'identification, le signataire est dument identifié.

604. Les fonctions d'authentification/identification[286] et de contrôle de l'intégrité sont inhérentes à la signature électronique fondée sur des clés asymétriques, ce que renseigne la loi n° 2000-230 du 13 mars 2000 pour reconnaitre la signature électronique.

---

[283] On nomme fonction de hachage, de l'anglais *hash function* (hash : pagaille, désordre, recouper et mélanger) par analogie avec la cuisine ; une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale. Les fonctions de hachage sont utilisées en informatique et en cryptographie.

[284] https://www.securiteinfo.com/cryptographie/hash.shtml.

[285] Il est à noter que le terme technique d'authentification est depuis longtemps employé dans les réglementations qui régissent la cryptologie. Outre cette fonction d'authentification, la cryptologie asymétrique permet également le contrôle d'intégrité du message, c'est-à-dire la possibilité d'établir que son contenu n'a pas été modifié.

[286] Voir *supra* n°499 s.

605. Pour conclure, lorsque nous signons un document numérique à l'aide d'une clé privée, nous chiffrons le document ainsi qu'un court extrait ; ensuite pour lire ce document rendu inintelligible par la clé privée, il faut avoir recours à une clé publique qui elle seule permet de déchiffrer le message.

B. Régime juridique de la cryptologie

1) Services de cryptologie en droit français

606. Le régime juridique des moyens et des prestations de cryptologie couvre une large palette de fonctions liées aux techniques de cryptologie. Des règles ont été établies pour encadrer l'activité de la prestation de ce type de services en renforçant la responsabilité des prestataires de services de cryptologie.

607. Depuis l'adoption de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), le principe de la liberté d'utilisation de tous les moyens de cryptologie est consacré en vertu de son article 30, quelle que soient les fonctions dudit moyen : confidentialité, authentification ou intégrité.

608. En France, les moyens de cryptologie sont soumis à une règlementation spécifique qui est prévue dans les articles 30 à 36 de la LCEN. D'après l'article 29 de la LCEN, nous entendons par moyen de cryptologie '*tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité'*.

609. En principe, l'utilisation d'un moyen de cryptologie est libre. Il n'y a aucune démarche à accomplir. Pourtant, la fourniture, l'importation, le transfert intracommunautaire et l'exportation d'un moyen de cryptologie sont soumis, sauf exception, à déclaration ou à demande d'autorisation. Ces démarches

incombent au fournisseur du moyen de cryptologie et sont à accomplir auprès de l'ANSSI[287].

610. Sauf exception, les démarches suivantes sont à accomplir pour toutes les opérations suivantes relatives aux moyens de cryptologie[288] :

Opération	**Démarches liées au « moyen de cryptologie » (par le fournisseur)**	**Démarches liées au classement « double usage » (par l'exportateur)**
Utilisation en France	/	/
Importation en France	Déclaration auprès de l'ANSSI	/
Fourniture en France	Déclaration auprès de l'ANSSI	/
Transfert intracommunautaire depuis et vers la France	Déclaration auprès de l'ANSSI	/
Exportation vers l'un des 7 pays « EU001 » (Australie, Canada, États-Unis d'Amérique, Japon, Nouvelle-Zélande, Norvège et Suisse)	Déclaration auprès de l'ANSSI	Demande d'autorisation générale de l'Union EU001 auprès du SBDU
Exportation vers un État tiers (hors UE et 7 pays « EU001 »)	Demande d'autorisation d'exportation auprès de l'ANSSI	Demande de licence d'exportation auprès du SBDU

611. D'ailleurs, la législation française distingue d'une part les fonctions d'authentification et d'intégrité des données, soumises à un régime libéral, ce qui est le cas de la signature électronique, aucune formalité préalable n'est exigée ; d'autre part il y a les fonctions de confidentialité, sur lesquelles l'Etat entend garder un contrôle étroit et nécessitera une déclaration ou une autorisation préalable du Premier ministre, mais son utilisation demeure libre[289].

[287] ANSSI signifie l' « Agence National de la Sécurité des Systèmes d'Information ».
[288] En ligne : https://www.ssi.gouv.fr/administration/reglementation/controle-reglementaire-sur-la-cryptographie/demarches-a-accomplir/.
[289] Valérie Sedallian, *Les problèmes posés par la législation française en matière de chiffrement, Droit de l'Informatique et des télécoms* 98/4 (10/98) [En ligne : http://encryption_policies.tripod.com/france/sedallian_1098_prob.htm].

612. Nous récapitulons le régime juridique des moyens de cryptologie (LCEN, article 30) dans le tableau suivant[290] :

Finalités du Moyen de Cryptologie	**Fonctions Offertes**			
	Authentification Intégrité (Signature électronique)		Confidentialité	
	Depuis un Etat membre de la Communauté européenne	Vers un Etat membre de la communauté européenne	Depuis un Etat membre de la Communauté européenne	Vers un Etat membre de la communauté européenne
Utilisation	Libre	Libre	Libre	Libre
Fourniture	Libre	Libre	Déclaration préalable au Premier ministre	Autorisation du Premier ministre
Transfert	Libre	Libre	Déclaration préalable au Premier ministre	Autorisation du Premier ministre
Importation	Libre	Libre	Déclaration préalable au Premier ministre	-
Exportation	-	Libre	-	Autorisation du Premier ministre

613. Les prestations de cryptologie consistent en toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie *(LCEN), art. 29), l'article 31* de cette même loi régit l'activité de fourniture de ce type de prestations.

614. La fourniture de prestations de cryptologie doit faire l'objet d'une déclaration auprès du Premier ministre dans des conditions définies par un décret en Conseil d'Etat[291]. Il précise que le même décret peut permettre la fourniture de certaines prestations sans formalité préalable compte tenu de leurs caractéristiques techniques ou de leurs conditions de fourniture.

[290] CAPRIOLI (E.), *Op. cit.*, p.218 s.
[291] Décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie.

615. Le paragraphe 2 de l'*article 31 de la LCEN* dispose que les personnes exerçant une activité de fourniture de prestations de cryptologie sont soumises au secret professionnel dans les conditions prévues aux *articles 226-13 et 226-14 du Code pénal*. Ces derniers articles du code pénal disposent qu'à l'exception des cas où la loi l'autorise ou l'impose, la révélation d'une information à caractère secret par une personne qui en est dépositaire est punie d'un an d'emprisonnement et de 15 000 euro d'amende.

616. Il est aussi important de noter que Le *décret n° 2007-663 du 2 mai 2007*[292] pris en l'application des *articles 30, 31 et 36 de la LCEN* et relatifs aux moyens et aux prestations de cryptologie et l'*arrêté du 25 mai 2007* définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et prestations de cryptologie sont venus préciser les formalités applicables en matière de cryptologie.

2) Services de cryptologie en droit européen

617. Les services et prestations de cryptologie ne sont pas traités dans le cadre de la proposition de règlement sur l'identification et les services de confiance. Cette réticence d'accorder une définition communautaire à la cryptologie est justifiée qu'il s'agit d'une branche des mathématiques qui est l'art de décrypter des messages chiffrés, un thème considéré technique qui n'exige pas l'intervention du législateur européen pour légiférer les prestations de cryptologie.

618. Aujourd'hui, et d'après les termes utilisés dans le règlement du Parlement européen et du Conseil du 23 juillet 2014, nous parlons plutôt de science de la confiance, étant donné sa diffusion de plus en plus répandue parmi les utilisateurs des réseaux numériques.

619. L'adoption du *règlement « eIDAS » n°910/2014 du 23 juillet 2014* fait suite à un relatif constat d'échec de la *directive 1999/93/CE* sur la signature

[292] *Ibid.*

électronique dont nous parlerons du contexte en détail lorsque nous envisageons les prestataires de services de confiance dans la prochaine section.

620. Faisons le constat suivant : la sécurité des transmissions électroniques ne peut être garantie que par une cryptographie forte. Le développement du commerce électronique qui par sa nature est international, suppose la possibilité de pouvoir importer et exporter librement des données cryptées. Il est donc important pour les documents électroniques d'avoir des normes techniques reconnues sur le plan international et permettre l'interopérabilité des systèmes[293].

621. Toutefois, ces besoins se heurtent à diverses restrictions à la libre exportation des produits de chiffrement. En effet, les produits de cryptographie font partie dans le commerce international des biens considérés comme « sensibles » ou « à double usage », c'est-à-dire les biens susceptibles d'avoir une utilisation tant civile que militaire.

622. Le régime de la cryptographie française concernant l'importation et l'exportation s'inscrit et doit respecter les exigences d'une réglementation européenne commune aux 15 Etats membres.

623. Il est d'ailleurs important de prendre en considération la réglementation américaine en matière d'exportation des prestations et des moyens de cryptologie en considération en raison de son impact et de l'importance des produits américains dans l'industrie informatique et le commerce électronique[294].

---

[293] En ce sens, voir *supra* n°1119.

[294] Aux Etats-Unis, il n'y a pas de restrictions concernant l'importation, l'utilisation et la fourniture des produits de cryptographie. En revanche, il existe une réglementation de l'administration fédérale concernant les exportations des « biens dits sensibles » qui trouve sa source dans l'*Export Administration Act*. Jusqu'à la fin 1996, les produits de chiffrement étaient classés dans la catégorie des munitions au sens de la loi américaine sur le contrôle et l'exportation des armes (*Arm Export Control Act*) et du décret sur le trafic international des armes (*ITAR, International Traffic in Arm Regulation*). Les produits de cryptographie étaient donc classés dans la catégorie des armes de guerre et munitions et leur exportation nécessitait une autorisation du département d'Etat et de la National Security Agency (NSA). Dans les années 90, sous la pression des entreprises, la tendance de l'administration américaine est d'assouplir le régime du contrôle des exportations, afin de faciliter le développement du commerce électronique. Par conséquent, depuis le 15 novembre 1996, le contrôle des exportations des produits de chiffrement relève de la compétence du *Commerce Department*, sauf pour les produits de chiffrement à des fins militaires qui restent de la compétence de l'ITAR. Le fait que les produits de chiffrement soient passés dans le champ d'application de

624. Suite à la consécration de la signature électronique, la *directive européenne 1999/93/CE du 13 décembre 1999* a opéré une distinction entre la signature ordinaire et la signature avancée. Cette classification a été maintenu lors de l'abrogation de la directive et retenu dans le règlement du Parlement européen et du Conseil du 23 juillet 2014.

625. D'une part, la signature ordinaire s'entend comme une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et sert de méthode d'authentification.

626. La signature ordinaire ne prouve pas l'identité du signataire. Elle permet simplement d'identifier la personne qui manipule ce dernier, sans pour autant pouvoir vérifier la qualité de l'émetteur[295].

627. Quant à la signature électronique avancée, elle est caractérisée par quatre exigences cumulatives énoncées à l'article 26 du règlement du 23 juillet 2014[296]. D'après l'article 26 du règlement du 23 juillet 2014 (repris de l'article 2.2 de la directive abrogée du 12 déc. 1999) la signature électronique avancée doit satisfaire aux quatre exigences suivantes:

a) être liée au signataire de manière univoque;

b) permettre d'identifier le signataire;

---

l'*Export Administration Act* ne signifie cependant pas la fin des contrôles à l'exportation. Si le département du Commerce attribue les licences d'exportation, les départements de la Justice, de l'Etat, de la Défense, de l'Energie, et les agences de contrôle des armes et du désarmement ont un droit de regard sur les licences accordées. Les entreprises du secteur informatique et les associations demandent constamment d'enlever ces restrictions imposées à la liberté de chiffrer et de lever les contrôles à l'exportation, et les années 2000 marquent un deuxième mouvement visant à l'assouplissement graduel du contrôle à l'exportation de la technologie cryptographique.

[295] En France, cette analyse de la signature ordinaire est retenue par la chambre sociale de la cour d'appel de Besancon, dans un arrêt du 20 octobre 2000 qui, dans le cas d'espèce, devait dire si un avocat pouvait valablement interjeter appel d'une décision prud'homale, en apposant une signature scannée au lieu et place de sa signature manuscrite. Les juges ont en effet souligné que la fiabilité du procédé utilisé en l'espèce par l'avocat est relative dans la mesure où le code permettant d'accéder à la signature peut être détenu par une autre personne du cabinet. CA. Besancon, ch. Soc., 20 oct. 2000, Chalets Boisson c/Gros, Expertises fevr. 2001. P.73, note Beaujard ; CCE janv. 2001, p.22, note Galloux ; *JCP* 2000, II, 10606, note Caprioli et Agosti – CONFIRMEE PAR Civ. 2e, 30 avr. 2003, n.00-46.467, *Bull.civ* II, n.118.

[296] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. [En ligne : http://data.europa.eu/eli/reg/2014/910/oj].

c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif; et

d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

628. Il résulte de ce texte que la signature avancée doit être liée uniquement au signataire, permettant de l'identifier, être créée par des moyens sous son contrôle exclusif, et être liée aux données auxquelles elle se rapporte, de telle sorte que toute modification ultérieure de ces données soit détectable.

629. A ces deux niveaux de signature, le *règlement du 23 juillet 2014* en ajoute une troisième : la signature électronique qualifiée. Cette dernière s'entend d'une « *signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié et qui repose sur un certificat qualifié de signature électronique* » (*article 3 (12) du règlement*).

630. Il est aussi prévu à l'alinéa 2 de l'*article 25* du règlement que « *l'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite* ». cette fiabilité technique de la signature électronique qualifiée en fait le fondement juridique et technique pour l'interopérabilité dans le marché européen de la confiance[297].

631. **– Conclusion intermédiaire** – Enfin, bien que ces services de cryptologie aient largement contribué à sécuriser le 'document transférable électronique', de nouveaux mécanismes de sécurité reposant sur l'externalisation des prestations informatiques ont été mis en place et connus un succès fulgurant ces dernières années: il s'agit des services '*Cloud computing*'.

[297] CAPRIOLI (E.) et AGOSTI (P.), « *La régulation du marché européen de la confiance numérique : enjeux et perspectives de la proposition de règlement européen sur l'identification électronique et les services de confiance », Communication Commerce électronique* n° 2, Février 2013, étude 3, n°12.

II. Nouveaux produits et services informatiques de sécurité des données électroniques

« L'informatique en nuages ou *Cloud computing* »

632. L'utilisation des technologies dans la société d'information a rendu nécessaire l'usage de moyens et des prestations de cryptologie, comme la protection de la confidentialité des données stockées sur un disque dur[298] ou sur clé USB ainsi que le secret des correspondances communiquées sur Internet, du secret des affaires et, bien entendu, du secret professionnel.

633. Cette protection de la confidentialité des données doit être assurée tout en maintenant la circulation de documents et autres échanges électroniques sur les réseaux sans pour autant être lues, altérées, détournées par des personnes non autorisées.

634. Il existe aujourd'hui des nouveaux produits cryptologiques efficaces pour assurer la sécurité et l'authentification des communications électroniques, disponibles sur le marché, nous présenterons les produits les plus fréquemment utilisés sur le marché ces dernières années.

635. Nous consacrerons cette section à la présentation et l'étude du phénomène "nuage", produit de sécurité par excellence sur le marché depuis cette dernière décennie. C'est le *Cloud computing* ou bien dans des termes français, nous l'appelons l'informatique en nuage.

636. Avant de démarrer l'étude sur l'informatique en nuage, il faut en premier lieu définir le produit cryptologique utilisé pour l'accès à des structures de type *Cloud computing*. Nous parlons ici de produit 'Réseau Privé Virtuel' (RPV), en anglais *Virtual Private Network* "VPN")

[298] http://www.vulgarisation-informatique.com/disque-dur.php.
Voir aussi : http://searchstorage.techtarget.com/definition/hard-disk.

637. Considéré aujourd'hui comme l'un des produits cryptologiques les plus fréquemment demandés par les utilisateurs pour assurer la sécurité et l'authentification des communications électroniques ; ces tunnels chiffrés (*vpn*)[299] sont utilisés surtout dans les grandes entreprises pour sécuriser leur base de données échangées[300].

638. En informatique, le *RPV* est un système permettant de créer un lien spécialisé direct entre des ordinateurs distants pour protéger les données échangées. Ce système utilise l'Internet comme support de transmission en utilisant un protocole d'"encapsulation" (en anglais tunneling, d'où l'utilisation impropre parfois du terme "tunnelisation"), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. Nous parlons alors de réseaux privés virtuels pour désigner le réseau ainsi artificiellement créé[301].

639. Ainsi la cryptologie et l'utilisation de réseaux privés virtuels peuvent garantir la confidentialité des communications électroniques, ainsi que d'identifier de manière certaine l'auteur d'un message et d'établir l'intégrité de celui-ci.

640. Théoriquement, bien que ca n'existe pas jusqu'à présent, rien n'empêche la possibilité de recours à la méthode *vpn* pour protéger les documents transférables électroniques, lorsque nous remplissons les deux critères de leur reconnaissance (i.e. l'intégrité et l'identification).

641. Pour conclure, le terme RPV est notamment utilisés par les grandes entreprises dans le travail à distance, ainsi que pour un moyen d'accès sécurisés à des structures de types *Cloud computing*.

---

[299] Pour savoir plus sur les VPN (réseaux privés Virtuels - RPV), veuillez consulter le lien suivant : http://www.commentcamarche.net/contents/514-vpn-reseaux-prives-virtuels-rpv.
[300] Eric A Caprioli, *Op. cit.*, p. 216 s.
[301] http://www.wefightcensorship.org/fr/article/virtual-private-network-vpn-ou-reseau-prive-virtuelhtml.html

1. Contexte historique du *Cloud computing*

642. Depuis l'année 2010, l'importance du service *Cloud computing* ou informatique en nuage ne cesse de grandir; le sujet est aujourd'hui « à la mode » dans le monde de l'informatique ; les grands prestataires de services investissent des sommes gigantesques sur le marché afin d'attirer les clients à adhérer aux services de *Cloud computing* leur appartenant.

643. Pourtant, le *Cloud computing* n'est pas apparu du jour au lendemain. L'idée appartient initialement aux années quatre-vingt avec l'émergence de l'externalisation des prestations informatiques et le développement de l'infogérance[302].

644. Puis, les années quatre-vingt-dix ont été marquées par la démocratisation de l'informatique dans les petites et moyennes entreprises (PME) et les très petites entreprises (TPE) avec l'informatique dite « personnelle ». Les années deux mille furent celles de l'Internet et des réseaux et c'est à partir de 2010 que nous trouvons la mobilité offerte par le *Cloud computing*.

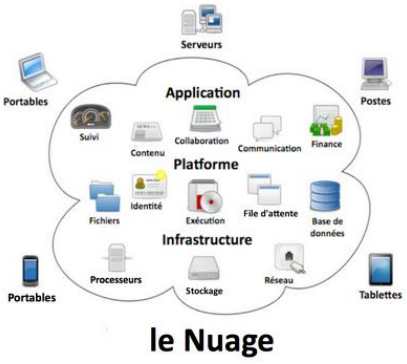

Figure 1 : Schéma représente la virtualisation et l'accessibilité par tout moyen de media

[302] L'infogérance est un cas particulier d'externalisation. Il s'agit d'un service défini comme le résultat d'une intégration d'un ensemble de services élémentaires, visant à confier à un prestataire informatique tout ou une partie du système informatique (SI) d'un client, dans le cadre d'un contrat pluriannuel, à base forfaitaire, avec un niveau de services et une durée définie (définition de l'AFNOR). En d'autres termes, c'est l'externalisation de tout ou partie de la gestion et de l'exploitation du SI à un prestataire informatique tiers (SSII nouvellement appelé ESN). Cette mission doit s'effectuer dans la durée et non de manière ponctuelle. [En ligne : http://www.internet-juridique.com/infogerance.php].

2. Notion de *Cloud computing* :

645. Il nous faut ici poser la question de savoir ce que l'on entend par *Cloud computing*, et quelle nouveauté il apporte au client.

a. Définition

646. Il y a de très nombreuses définitions pour le *Cloud computing*. Nous nous contentons de présenter celles qui sont proposées par les plus grands fournisseurs dans le secteur de la technologie informatique.

647. D'abord, une définition générale de *Cloud computing* est prévue par le Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (*cloud computing*)[303]. Il précise qu'il s'agit d'un *modèle permettant un accès aisé, à la demande et au travers d'un réseau, à un ensemble partagé de ressources informatiques.*

648. *Cisco*, fournisseur de réseau, définit le *Cloud computing* comme des « *ressources informatiques et des services abstraits de l'infrastructure sous-jacente et fournis à la demande et à l'échelle dans un environnement partagé* »[304].

649. Une autre définition proposée par le fournisseur d'applications *Microsoft* prévoit qu'il s'agit de « *l'ensemble des disciplines technologiques et modèles commerciaux utilisés pour délivrer des capacités informatiques (logiciels, plateformes, matériels), comme un service à la demande. Ce service comporte cinq caractéristique clés : le service est à la demande, le service est accessible n'importe où grâce aux réseaux, le service est mesuré, la quantité est modulable offrant une élasticité infinie, les ressources sont mises en commun ce qui réduit les coûts* »[305]

---

[303] « Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (*cloud computing*) - référentiel d'exigences», version 1.3, 30/07/2014, *Agence nationale de la sécurité des systèmes d'information,* [En ligne : http://www.ssi.gouv.fr/uploads/IMG/pdf/cloud_referentiel_exigences_anssi.pdf]

[304] http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/CiscoCloudComputing_WP.pdf.

[305] https://blogs.technet.microsoft.com/itinsights/2010/12/07/how-microsoft-defines-cloud-computing/.

650. En France, le *Cloud computing* est défini par la Commission générale de terminologie et de néologie précise, en prévoyant qu'il s'agit d'*une forme particulière de gérance de l'information, dans laquelle l'emplacement et le fonctionnement dans le nuage ne sont pas portés à la connaissance des clients*[306].

651. Le *National Institute of Standards Technology (NIST)*[307] a présenté une définition fréquemment utilisée. Le NIST le définit comme : *« un modèle proposant un ensemble de ressources partagées (réseaux, serveurs, stockage, applications et services numériques) accessible partout et à la demande à travers le réseau et qui peut être rapidement alloué et libéré avec un minimum de maintenance ou d'interaction avec le fournisseur du service* ».

652. Pour simplifier la notion, l'idée de base du *Cloud computing* est la suivante: pour éviter au client toute installation supplémentaire sur son ordinateur et de consommer un ensemble de "ready-to-use" (prêt à l'emploi structuré), des services informatiques Web, les logiciels et les données ("le nuage"), sont offerts via un navigateur Web, sans aucune exigence supplémentaire pour les ordinateurs du client Cloud. Seul un ordinateur avec un système d'exploitation, un navigateur Web, et un 'accès à Internet est nécessaire pour le client désirant utiliser la puissance du *cloud computing*[308].

653. En d'autres termes, le *Cloud computing* est un mode de gestion virtualisée des infrastructures, des équipements mais aussi des logiciels et applications dont l'exploitation s'effectue de manière dématérialisée sous la forme de services distants fournis à ses clients par un prestataire via Internet.

---

[306] Avis et Communications, Vocabulaire de l'informatique et de l'internet, *JORF* n°0129 du 6 juin 2010 page 10453 texte n° 42.
[En ligne : https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000022309303].

[307] [En ligne : http://www.nist.gov], et pour une définition du cloud computing : [En ligne : https://www.nist.gov/itl/cloud-computing] : "*Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*".

[308] Vladimir O. Safonov, *Trustworthy Cloud Computing, Edition John Wiley and Sons*, Fevrier 2016.

654. Techniquement, cette approche est très innovante, car elle change radicalement la perspective du développeur de logiciels sur l'utilisation des ressources. Au lieu du temps et des démarches longues et ardues du passé, telles que: « Je vais installer tels ou tels logiciels et telles données sur mon ordinateur pour résoudre certaines tâches (l'installation peut nécessiter plusieurs jours, et parfois une mise à niveau/ actualisation importante ou même un remplacement de l'ordinateur pourrait être nécessaire)", le client peut désormais utiliser l'approche « nuage » moderne. Dans ces conditions le client raisonne différemment « Je souscris aux services *cloud* de la société X pour six mois et résoudrai avec l'aide des ressources de cloud tous mes problèmes, j'utilise le « nuage » quand et où je veux, source de confort de travail en me connectant sur Cloud depuis mon *smartphone* ou mon ordinateur portable. "

655. La différence est marquante entre ces deux approches. En raison de l'utilisation du nuage, l'utilisateur est libéré du travail technique de routine et qui ne relève pas de ses compétences, pour passer à l'activité créatrice.

656. Dans une perspective juridique, toutes les définitions de *Cloud computing* peuvent laisser perplexe ; ce concept soulève de nombreuses préoccupations juridiques qu'il convient d'anticiper, lorsqu'on parle du mécanisme de *Cloud computing*. En effet ce système repose sur le recours à l'externalisation des prestations informatiques sans se soucier des difficultés relatives à la protection juridique des données privées et au partage des documents informatiques.

657. Pour saisir le concept du *Cloud computing*, nous citons l'exemple classique d'un prestataire de services informatique qui propose ses produits et services par le biais de licences associées de contrats de maintenance et, le cas échéant, de contrats de développements et/ou de services. En utilisant le service *Cloud*, ce même prestataire informatique peut offrir les mêmes produits et services au travers d'un accès de type « SaaS » (software as a service) dont nous allons présenter la signification[309].

[309] Voir *supra* n°675 s.

658. Dans la première hypothèse de prestation classique de services informatiques, le client installe ou fait installer les applications[310] dont il a besoin sur ses équipements ou ceux dont il a la disposition chez son prestataire d'hébergement ; par contre dans l'hypothèse de la prestation de services *Cloud*, les logiciels seront directement accessibles par le client après authentification via Internet sans avoir besoin de les installer sur leurs équipements.

659. Le prestataire de service informatique assume la responsabilité de garantir l'intégrité des documents électroniques ainsi que la confidentialité des toutes informations partagée sur le service *Cloud computing*.

b. Traits caractéristiques du *Cloud computing*

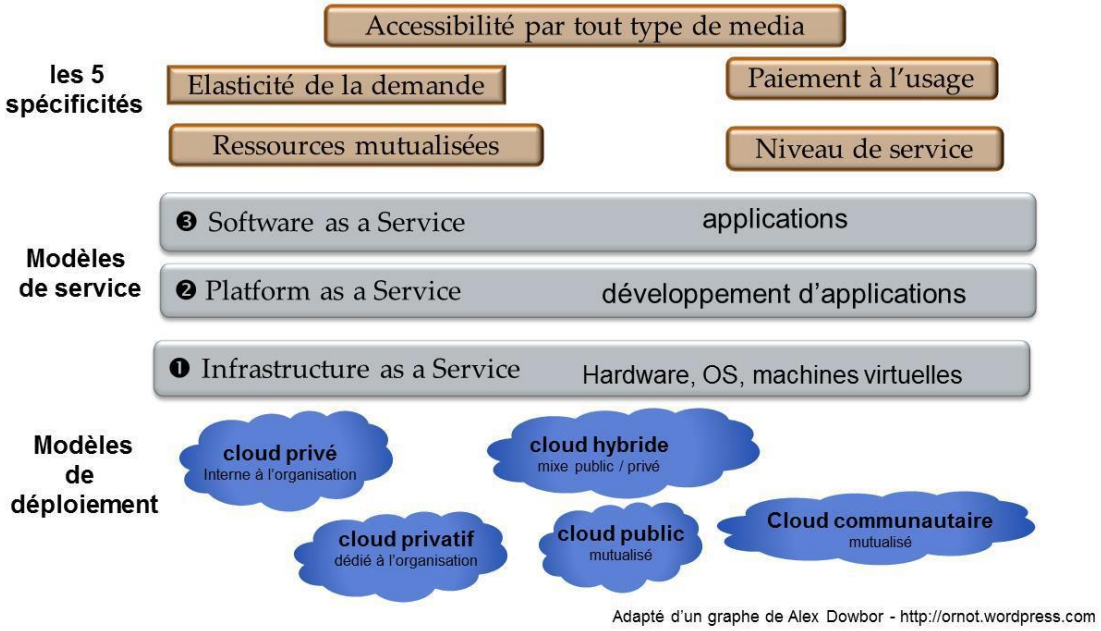

Figure 2 : schéma synthétise les spécificités, les modèles de service et les modèles de déploiement *Cloud.*

660. Le recours au *Cloud computing* présente des avantages quand nous le comparons avec le moyen traditionnel de vente de "License et services

[310] Application est un terme informatique qui signifie un programme ou ensemble de programmes destiné à aider l'utilisateur d'un ordinateur pour le traitement d'une tâche précise.
[En ligne : http://www.larousse.fr/dictionnaires/francais/application/4707].

associés"[311]. D'abord, il permet une mise à jour en continu et automatique des applications. Le client n'a plus besoin de demander la mise à jour des applications chaque fois qu'il y a une nouvelle version sur le marché, le prestataire de services s'occupera désormais de la mise à jour des services informatiques inclus dans le contrat. Ainsi le client dispose, pendant toute la période du contrat, des équipements mis à jour automatiquement et prêts à l'usage.

661. Par conséquent, le *Cloud computing* est avantageux pour le client dans la mesure où il réduit et rationnalise les coûts, en supprimant d'une part les équipements nécessaires à la mise en œuvre des logiciels et, d'autre part les frais de maintenance associés.

662. Ensuite, il est présenté comme visant, par une approche « *pay as you go* » (c.à.d. Payez ce que vous consommez)[312] ; cette option signifie que le client paie le prestataire de services informatiques au fur à mesure de sa consommation du service *Cloud computing*[313].

663. Pendant ces dernières années où il y a de forte tension sur les budgets partout dans le monde des affaires, le *Cloud computing* rencontre un succès considérable lorsque son utilisation se paie à l'usage, ce qui donne l'impression qu'il est moins cher[314]

664. Il faut d'ailleurs préciser que le *Cloud computing* est considéré comme une charge récurrente, et non un investissement ; d'un point de vue comptable, le coût d'accès à un des services proposés en Cloud constituera une charge

---

[311] *Dans un contrat de vente de licence en général, nous parlons d'un logiciel qui est "vendu" comme un bien destiné uniquement à être utilisé par une entreprise dans ses fonctions de base, même avec des adaptations, cas dans lesquels la propriété littéraire et artistique n'entre absolument pas en ligne de compte. Dès l'acceptation du client de la commande par le vendeur, ce dernier lui est concédé un droit (selon les cas, exclusif ou non exclusif, cessible ou non cessible) d'utilisation des logiciels et des services commandés, pour la durée de protection par le droit d'auteur. Dans ce sens, voir :* Guillaume Blanc-Jouvan, « *Fasc. 321 : Fourniture d'un logiciel ou d'un progiciel*», LexisNexis, 20 Avril 2009, n°17 s.

[312] Barrie Sosinsky, *Cloud Computing Bible*, John Wiley & Sons, January 11, 2011, p.17 s.

[313] Emmanuel SORDET et Richard MILCHIOR, *Le Cloud computing, un objet juridique non identifié ?*, Communication Commerce électronique n° 11, Novembre 2011, étude 20.

[314] Isabelle Renard, *3 QUESTIONS Le Cloud Computing*, La Semaine Juridique Entreprise et Affaires n° 50, 13 Décembre 2012, 770.

d'exploitation quand le recours à des licences et à l'équipement nécessaire pour les faire fonctionner se traduira par la constatation au bilan d'immobilisations[315].

665. Enfin, d'un point de vue plus technique, le Cloud computing permet une mutualisation et une allocation dynamique de capacité (c.-à-d. des ressources de stockage et de traitement) en fonction des besoins de l'entreprise suivant ainsi ses cycles de développement.

666. Les ressources sont mutualisées et virtualisées, qu'elles soient matérielles ou logicielles, permettent le déploiement des solutions de façons indistinctes sur différents matériels formant ainsi une ressource globale.

667. Citons l'exemple d'une entreprise qui voulait transmettre les solutions et ressources logicielles qu'il dispose dans sa nouvelle filiale. Pour ce faire, il fallait dépenser une somme considérable afin de pouvoir effectuer une telle tache et mettre en œuvre les mêmes solutions dans cette nouvelle entité. Grâce à la virtualisation dans le Cloud computing, le transfert des solutions s'effectue simplement en cliquant sur le clavier et en suivant quelques étapes sur le système pour effectuer la mutualisation des ressources dans la nouvelle filiale.

668. Nous comprenons dès lors l'intérêt pour les entreprises de recourir au *Cloud computing*.

3. Types de *Cloud computing*

669. Il existe plusieurs modes de *Cloud computing* dont les trois principaux à ce jour sont le SaaS (Software as a service), le PaaS (Platform as a service) et l'IaaS (Infrastructure as a service), la forme originelle du *Cloud computing*. Alors que le SaaS permet l'accès aux données via Internet, le PaaS facilite le développement d'applications. Quant à l'IaaS, il s'agit d'une infrastructure fournissant des capacités de traitement.

[315] Emmanuel SORDET et Richard MILCHIOR, *Op. cit.*

Les différentes activités de *Cloud* se présentent dans l'ordre suivant :

a. Fourniture de service **IaaS** (*Infrastructure as a service*)

670. Cette offre concerne la mise à disposition de ressources informatiques (puissance CPU, mémoire, stockage etc.). Le modèle IaaS permet au client de disposer de ressources externalisées virtualisées. Celui-ci garde le contrôle sur le système d'exploitation (OS), le stockage, les applications déployées ainsi que sur certains composants réseau (pare-feu, par exemple).

671. Le *IaaS* consiste à mettre dans le *Cloud* des serveurs partagés virtualisés, avec le système d'exploitation, et vendus à la demande. Ils sont généralement vendus selon des métriques liées au nombre de sessions virtuelles, la quantité de mémoire allouée, l'espace de stockage utilisé ainsi que le débit réseau utilisé.

672. Ainsi lorsque par exemple un client souhaite avoir plus d'espace, il paiera pour les sessions virtuelles demandées ; et lorsqu'il a besoin de plus de vitesse pour effectuer ses taches, il demande l'augmentation de la quantité de mémoire allouée.

b. Fourniture de service **PaaS** (*Platform as a service*)

673. Cette offre concerne la mise à disposition de plates-formes de *middleware*, de développement, de test, d'exécution d'applications. Le *PaaS* correspond à la partie Middleware. Les *middlewares* sont les bases de données, les serveurs web, les serveurs d'application, les environnements de développement. Un environnement *PaaS* consiste donc à proposer à l'usage ces outils sur un environnement en mode *IaaS*.

674. Ici le prestataire gère et contrôle l'infrastructure technique (réseau, serveurs, OS, stockage, etc.). Le client est responsable du déploiement des applications et de leur paramétrage

c. Fourniture de service **SaaS** *(Software as a service)*

675. Cette dernière catégorie d'offre concerne la mise à disposition d'applications d'entreprise : outils de gestion de la relation client, outils collaboratifs, messagerie, *Business Intelligence*, outils de gestion intégrés, etc.

676. Le *Saas* a pour but de proposer une application complète qui doit être plus ou moins personnalisée pour le client. L'application proposée dispose d'une interface utilisateur, d'une interface pour le manager et les utilisateurs. Ces applications sont souvent proposées selon des métriques business : nombre d'utilisateurs, nombre de transactions etc… Les offres sont très nombreuses et dans tous les domaines mais principalement des domaines transverses pour le moment.

677. Quant à la gestion du service SaaS, c'est le prestataire qui offre une fonction opérationnelle et gère de façon transparente pour l'utilisateur l'ensemble des aspects techniques requérant des compétences informatiques. Le client garde quand même la possibilité d'effectuer quelques paramétrages de l'application.

678. Suite à cette présentation brève de différents types de *Cloud Computing*, nous apercevons qu'il s'agit effectivement d'une forme de distribution d'« énergie informatique » qui permet de s'affranchir des contraintes liées à la gestion d'une informatique interne.

679. L'idée n'est pas nouvelle : il est depuis longtemps possible d'externaliser tout ou partie de son informatique à un prestataire et ce, que ce soit au niveau de l'infrastructure de base (« IaaS »), de la plate-forme (« PaaS ») ou encore de l'application (« SaaS »). Mais le *Cloud Computing* diffère de l'infogérance classique par son caractère « distribué » des infrastructures (c'est-à-dire la répartition de la puissance informatique sur des centres de calcul géographiquement distants reliés par des réseaux à haute vitesse).

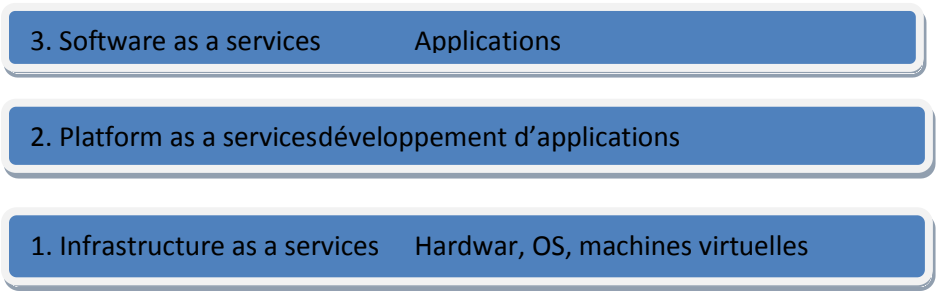

Figure 3 : nous illustrons les différents modèles de service *Cloud* comme des couches technologiques

680. Ce schéma 3 fait l'illustration des différents modèles de service *Cloud computing*, et que chacun de ses services donne des prérogatives aux clients par rapport à son niveau.

4. Modèles de déploiement

681. Une autre distinction importante à signaler, selon qu'il existe un réseau Internet ouvert au public ou un réseau intranet réservé aux collaborateurs et tiers autorisés d'une entreprise : le Cloud public et le Cloud privé[316].

682. Dans le premier, le prestataire met à disposition de ses clients un accès à ses services en libre-service alors que, dans le second, il va constituer pour un client donné un espace dédié et sécurisé. Il existe aussi un Cloud hybride qui combine ces deux modes d'accès ainsi qu'un Cloud communautaire, lequel est partagé par des clients ayant des intérêts ou un projet commun.

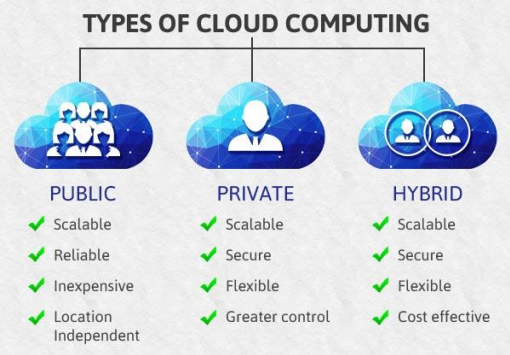

Figure 5 : les différents modèles de déploiement *Cloud*

[316] Barrie Sosinsky, *Op. cit.*, p.7 s.

683. Face à l'émergence de l'information dans les *nuages ou Cloud computing*, associée aux services proposés en mode *SaaS (software as a Service)*, nous pouvons théoriquement envisager le recours au service *Cloud computing* pour les documents transférables par voie électronique, lorsqu'il existe une garantie de la conformité juridique des opérations, spécialement le contrôle et le suivi des identités des utilisateurs de ces services ; la confiance passe par la mise en place de méthodes d'authentification (comme par exemple le système *Single Sign-on* "*SSO*", *OTP*, certificats). La sécurité et la confidentialité des informations, ainsi que leur lieu d'hébergement sont des questions clés notamment en termes contractuels[317].

684. **– Conclusion intermédiaire** – Les différents services de sécurité et de prestations de service informatique sont fournis par des prestataires de confiance ; ces derniers prennent en charge la gestion de données pour le compte des usagers, en garantissant l'exactitude des documents et la signature électronique.

[317] Eric A Caprioli, *Op. cit.*, p.22 s.

SECTION II : LES PRESTATAIRES DANS LE SERVICE DE CONFIANCE : LES GARANTS DE LA SIGNATURE

685. En France, le *décret n° 2001-272 du 30 mars 2001* sur la signature, pris en application de l'*article 1316-4 du code civil* envisage le tiers de confiance en tant que prestataire de services de certification.

686. Selon l'*article 6* du décret précité, nous trouvons diverses indications relatives au prestataire de services de certification, au signataire et à des données qui lui sont propres (début et fin de validité, limites d'utilisation et limites à la valeur des transactions pour lesquelles il peut être utilisé, …).

687. Pourtant depuis la mise en application du *Règlement européen du 23 juillet 2014*, nous parlons désormais du prestataire de services de confiance, plutôt que de limiter le champ d'application aux seuls prestataires de services de certification.

688. Contrairement à la *directive 1999/93/CE* qui se limitait à réglementer la signature électronique et les prestataires de service de certification, le *Règlement du 23 juillet 2014* couvre d'autres services de confiance, ainsi que les prestataires qui les offrent, tels que le cachet, l'horodatage, le service d'envoi recommandé électroniques et l'authentification de site Internet.

689. Cette extension nous parait logique. Une législation qui se limite à l'intervention du tiers de confiance dans le cadre de la signature électronique et les certificats d'identité n'avait pas de sens. Un tiers de confiance peut avoir d'autres champs d'intervention lorsque nous envisageons la conclusion, la transmission et la conservation d'un acte juridique dans un processus complètement électronique.

690. Dans un premier temps nous présentons les prestataires de service de confiance, leur attribuer une définition et d'exposer leurs critères de qualification (Paragraphe I), ensuite nous envisageons les obligations et responsabilité des prestataires de service de confiance (Paragraphe II). Dans un troisième et dernier temps, nous exposons un exemple significatif de prestation de service de confiance qualifié, qui est la prestation de services d'horodatage (Paragraphe III).

PARAGRAPHE I PRÉSENTATION DES PRESTATAIRES DE SERVICE DE CONFIANCE

691. Le prestataire de services de confiance joue un rôle prépondérant pour établir la confiance des usagers dans le domaine du commerce électronique. La confiance numérique repose principalement sur différents facteurs : ceux qui sont d'ordre physique, tels que la fiabilité des matériels et logiciels, et ceux d'ordre humain comme l'organisation des prestataires en charge d'un service de confiance.

692. Afin d'assurer le développement durable du réseau, plusieurs techniques permettent de gagner la confiance des utilisateurs d'Internet. Ces techniques impliquent parfois le recours à un tiers (autorité de certification, horodateur, archiveur, labellisateur, etc.), dont le métier est précisément d'intervenir afin de créer, d'une autre manière que dans l'environnement traditionnel, un environnement dans lequel les transactions peuvent s'opérer en toute confiance et de manière sécurisée. Nous voyons ainsi se développer ce que certains ont baptisé il y a 15 ans déjà les « nouveaux métiers de la confiance »[318].

693. Ainsi la confiance dépend désormais des tiers ; ces intermédiaires qui sont les prestataires de service de confiance. S'agissant de nouveaux métiers de confiance, le droit reconnait progressivement leur intervention afin de renforcer la confiance entre les usagers. Si la confiance ne peut naître du seul rapport

[318] M. ANTOINE, D. GOBERT et A. SALAÜN, *Le développement du commerce électronique : les nouveaux métiers de la confiance », in Droit des technologies de l'information, regards prospectifs*, *Cahiers du CRID*, n° 16, Bruxelles, Bruylant, 1999, p. 3 à 32.

entre les parties, cela ouvre le champ à l'intervention des tiers dont l'activité est de créer, de manière originale, les éléments de la confiance et de la sécurité.

I. Qualification des prestataires de service de confiance

A. Notion des prestataires de service de confiance

694. Au sens de l'*ordonnance n° 2005-1516 du 8 décembre 2005* relative aux échanges par voie électronique, un prestataire de services de confiance est défini comme « *toute personne offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique* ». Cette définition nous montre que l'élément humain dans une transaction par voie électronique est très important dans le sens où faire confiance à un service revient avant tout à faire confiance à celui qui fournit ce service et comment ce dernier le gère comme moyen de garantir la sécurité escomptée des informations échangées par voie électronique.

695. Au niveau européen, le *Règlement européen du 23 juillet 2014* [319] attribue aussi une définition similaire aux prestataires de services de confiance[320] ; la fiabilité de leurs pratiques ou de leurs produits étant reconnue par chaque Etat membre. Le règlement du 23 juillet 2014 a élargi le champ d'application des services de confiance qui regroupe désormais de nombreux services, et les prestataires de services de confiance pourront ainsi agir dans plusieurs domaines d'activités bien que leur régime juridique ne soit pas unifié.

696. Afin de matérialiser cette confiance, certaines conditions doivent être respectées dans le but d'auditer et vérifier la qualité du service fourni. Nous parlons ici de la conformité, de la qualification, de certification, de référencement des prestataires par rapport à un état de l'art normatif particulier.

[319] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, [En ligne : http://data.europa.eu/eli/reg/2014/910/oj].

[320] D'après l'article 3 (19) du Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014, le «prestataire de services de confiance» est une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié

697. Toutes ces procédures de contrôle susmentionnées visent à amplifier et rejaillir le sentiment de confiance de la part des usagers et les internautes. Un prestataire de service fiable doit être doté de la spécialisation et un certain niveau de professionnalisme dans le cadre de l'exercice de son métier. En procédant de la sorte, la confiance des usagers exige que le rôle des prestataires de service contribuant à des transactions par voie électronique soit clairement spécifié et bien encadré dans leur domaine d'intervention.

698. D'ailleurs, le régime juridique des prestataires de services de confiance (PSC) ne doit pas être réduit ni confondu avec la notion de « *tiers de confiance* » ; cette notion de « *tiers de confiance* » a été introduite dans le *décret n° 2011-1997 du 28 décembre 2011* relatif au dispositif de « tiers de confiance » prévu à l'*article 170 ter du Code général des impôts*[321]. En effet cette définition de « *tiers de confiance* » ne relève pas de notre sujet, car l'*article 170 ter du* Code *général des* impôts prévoit que, « *la mission de tiers de confiance est réservée aux personnes membres des professions réglementées d'avocat, de notaire et de l'expertise comptable* ».

La notion de « tiers de confiance » qui relève de notre sujet se présente dans un sens plus large et qui s'étend aux prestataires qui agissent sur les réseaux numériques, assurant plusieurs rôles primordiaux à la confiance des usagers, tels que la signature, les certificats, la datation électronique, la gestion de la preuve et sa validation, l'archivage et la cryptologie.

B. <u>Les aspects caractéristiques du prestataire de services de confiance.</u>

699. Ces aspects peuvent être introduits dans l'ordre suivant :

i. **La fiabilité du tiers de confiance** : la sécurité technique des tiers de confiance dépend essentiellement de la qualité des technologies adoptées par les

[321]Article 170 ter, II) du Code général des Impôts prévoit que « La mission de tiers de confiance est réservée aux personnes membres des professions réglementées d'avocat, de notaire et de l'expertise comptable », [En ligne : https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000024189377&cidTexte=LEGITEXT000006069577].

prestataires de service. La fiabilité de la technologie et services peut être soutenue et assurée par certaines mesures de sécurité : comme la qualification, certifications des services ou matériels (auprès de l'Agence National de la Sécurité des Systèmes d'Information « ANSSI »[322]) ou encore des labellisations CNIL[323] et celle de l'Union européenne pour les services qualifiés (cette labellisation sera présentée plus tard dans le deuxième paragraphe de la présente section).

ii. **La mise en œuvre des processus technologique automatisés** : la technologie utilisée par le prestataire de services de confiance doit être mise en œuvre dans la mesure où la production des documents numériques s'effectue avec le moins d'interactions possible avec une personne physique, susceptible de modifier le contenu d'un service. Cette automatisation des processus sert aussi à faciliter la traçabilité des opérations intervenues dans le cadre du service.

iii. **La pérennité de l'entité**. Il est important que l'activité du tiers de confiance soit durable et pérenne dans le temps avec une base financière solide.

iv. **L'impartialité du tiers de confiance et la possibilité de recours aux prestataires externes** : par définition, l'"impartialité" est une qualité exigée dans un juge ou un arbitre pour qu'il soit indépendant au regard de l'autorité de l'Etat et pour qu'il soit neutre à l'égard des parties au litige[324].

700. Pour un prestataire de service, étant partiel n'exige pas forcement le caractère externe. Bien qu'il nous semble pourtant vrai que le recours à un tiers externe puisse constituer une précaution satisfaisante assurant son indépendance, la notion de prestataire de service ne renvoie pas exclusivement à l'idée d'externalisation.

[322] L'Agence National de la Sécurité des Systèmes d'Information (ANSSI) est un service français créé par décret le 7 juillet 2009. Ce service à compétence nationale est rattaché au Secrétaire générale de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. [En ligne : http://www.ssi.gouv.fr/].

[323] La notion de labellisation est comprise par le grand public comme étant un mode de reconnaissance d'un niveau de qualité, conformément à l'état de l'art du marché et aux bonnes pratiques, délivrée par une entité privée ou une autorité publique, adossée à un cahier des charges.

[324] L'"impartialité" est définie comme la règle selon laquelle il convient que les juges et les arbitres soient indépendants au regard l'autorité de l'Etat et neutres à l'égard des parties. Dictionnaire en ligne du Droit Privé, [En ligne : http://www.dictionnaire-juridique.com/definition/impartialite.php].

701. Le droit français prévoit les deux possibilités soit d'internaliser ou d'externaliser la fonction du prestataire de services de confiance dans un texte. Il s'agit de l'article 19 du *décret n° 2010-112 du 2 février 2010*[325] pris pour l'application des articles 9, 10 et 12 de l'*ordonnance n° 2005-1516 du 8 décembre 2005* ; ce texte prévoit clairement ces deux possibilités, admettant la possibilité pour une autorité administrative d'agir comme prestataire de services de confiance pour ses besoins propres ou au profit d'autres autorités administratives.

702. **– Conclusion intermédiaire** – Alors, ces tiers de confiance doivent être suffisamment compétents pour pouvoir fournir les différents services de confiance aux usagers. Ils sont assujettis à certains règles de contrôle, et éventuellement être qualifiés dans leur domaine d'intervention.

II. PROCÉDURE DE CONTRÔLE ET DE CONFORMITÉ DANS LE CADRE DES PRESTATAIRES DE SERVICES DE CONFIANCE

703. En droit français, l'*ordonnance du 8 décembre 2005*[326] met en œuvre des procédés pour les transmissions électroniques en général. Ces outils retenus par l'ordonnance sont définis comme *"tout dispositif, matériel ou logiciel, mettant en œuvre des fonctions qui contribuent à la sécurité des informations échangées par voie électronique"(article 1er, II, 3°).*

704. Ce texte précise que les fonctions qui contribuent à la sécurité sont occupées par les prestataires de services de confiance et que c'est à ces derniers d'offrir leurs services afin de mettre en œuvre ces fonctions d'assurer la sécurité

[325] Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, [En ligne : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&categorieLien=id].
[326] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, [En ligne : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232].

des informations échangées par voie électronique *(article 1er, II, 2° dudit ordonnance).*

705. Pour rendre le choix plus simple pour les administrations de choisir les prestataires de service, ils ont à leur disposition certains outils élaborés à cette fin: on parle ici de "référentiels" de sécurité, d'interopérabilité et d'accessibilité.

706. Ainsi il s'agit à la fois de choisir des référentiels (A) et un système de certification (B).

A. Le système de référentiels

707. En 2014, L'Agence Nationale de la Sécurité des Systèmes Informatiques (ANSSI) a été désignée par les autorités françaises comme l'organe de contrôle, c'est-à-dire l'organisme en charge de délivrer et de retirer les qualifications des prestataires de services de confiance.

708. A ce titre, l'ANSSI publie des référentiels d'exigences applicables aux différents services de confiance. La notion de référencement renvoie au Référentiel général de sécurité prévue à l'article 9 de l'ordonnance du 8 décembre 2005[327].

709. Dans ce texte, nous retenons qu'un prestataire de services de confiance doit disposer des compétences, et les moyens techniques nécessaires à obéir aux fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique ; en accomplissant ces taches, le prestataire de

[327] Article 9 de l'ordonnance du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives prévoit que :
«I. - Un référentiel général de sécurité fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité et d'horodatage. Les conditions d'élaboration, d'approbation, de modification et de publication de ce référentiel sont fixées par décret.
II. - Lorsqu'une autorité administrative met en place un système d'information, elle détermine les fonctions de sécurité nécessaires pour protéger ce système. Pour les fonctions de sécurité traitées par le référentiel général de sécurité, elle fixe le niveau de sécurité requis parmi les niveaux prévus et respecte les règles correspondantes. Un décret précise les modalités d'application du présent II.
III. - Les produits de sécurité et les prestataires de services de confiance peuvent obtenir une qualification qui atteste de leur conformité à un niveau de sécurité du référentiel général de sécurité. Un décret précise les conditions de délivrance de cette qualification. Cette délivrance peut, s'agissant des prestataires de services de confiance, être confiée à un organisme privé habilité à cet effet ».

services de confiance pourra obtenir la qualification lui permettant d'agir et exercer librement ses activités sur le marché, de manière favorable par rapport à un autre prestataire non qualifié.

710. En droit français, ce référencement d'un produit de sécurité ou d'un prestataire de services de confiance s'effectue sur la base d'un cahier des charges qui précise les règles de sécurité et d'interopérabilité à respecter et, conformément au décret n° 2010-112 du 2 fév. 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 déc. 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et à l'arrêté du 18 janvier 2012 relatif au référencement de produits de sécurité ou d'offres de prestataires de services de confiance.

711. Ainsi, le référencement s'effectue en rapport à des fonctions de sécurité telles que l'authentification, ou la signature, et un niveau de sécurité tels que décrits dans le Référentiel général de sécurité.

a) Référentiel Général de Sécurité (RGS)

i. Contexte

712. Le Référentiel général de sécurité (RGS) a pour objectif principal de sécuriser les échanges administratifs, et comporte un cadre de règles que doivent respecter les fonctions des systèmes d'information développés par les administrations, en ce qui relève de l'identification, de la signature électronique, la confidentialité et l'horodatage.

713. Ce référentiel est prévu initialement par l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, puis il été adopté par le décret n° 2010-112 du 2 février 2010[328] pris pour l'application des articles 9, 10 et 12 de l'ordonnance précitée relative à la sécurité des informations échangées par voie électronique.

[328] D. n° 2010-112, 2 févr. 2010 *fixant les conditions d'élaboration et de publication du Référentiel général de sécurité : Journal Officiel* 4 Février 2010, p. 2072. - *A. 6 mai 2010, portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certifications électroniques : Journal Officiel 18 Mai 2010.*

714. La deuxième version du RGS est publiée par l'arrêté du 13 juin 2014[329] portant approbation du référentiel général de sécurité et précisant les modalités pour mettre en œuvre la procédure de validation des certificats électroniques.

715. Cette dernière version du référentiel remplace la première version du RGS publiée par arrêté du Premier ministre le 6 mai 2010. Elle a apporté des modifications à la première version, en complétant les règles et les recommandations relatives aux certificats électroniques et contremarques de temps et permet la qualification des prestataires d'audit de la sécurité des systèmes d'information.

716. Nous signalons aussi que la transition des certificats vers la nouvelle version du référentiel s'effectue normalement pendant l'année qui suit l'entrée en vigueur de la nouvelle version 2014 lorsqu'ils étaient conformes aux dispositions de la première version du RGS[330].

ii. Champ d'application du RGS.

717. Par défaut, ce référentiel s'applique à l'ensemble des autorités administratives visées par l'article 1er, I de l'ordonnance de 2005, ainsi qu'aux prestataires de services, aux fournisseurs de produits de sécurité et aux usagers.

718. Ainsi le RGS s'impose spécifiquement aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et dans leurs relations avec les usagers.

719. D'ailleurs, le RGS s'adresse indirectement à l'ensemble des prestataires de services qui assistent les autorités administratives dans la sécurisation des

[329] Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques. [En ligne : https://www.legifrance.gouv.fr/eli/arrete/2014/6/13/PRMD1413745A/jo/texte].

[330] Le chapitre 8 du RGS en date de 13 juin 2014 prévoit les mesures transitoires suivantes : "*les certificats conformes aux annexes de la première version du RGS pourront encore être émis pendant l'année qui suit l'entrée en vigueur de la présente version. Les autorités administratives devront accepter ces certificats pendant leur durée de vie jusqu'à concurrence de trois (3) ans, soit au maximum pendant les quatre (4) années qui suivent l'entrée en vigueur de la présente version du référentiel général de sécurité ; les certificats conformes aux annexes de la présente version pourront être émis à compter de son entrée en vigueur. Les autorités administratives devront accepter ces certificats au plus tard un (1) an après cette date*".

échanges électroniques qu'elles mettent en œuvre, ainsi qu'aux industriels dont l'activité est de proposer des produits de sécurité.

720. Le champ d'application n'est pas finalement réservé aux autorités administratives, le RGS peut en général s'appliquer à tout organisme souhaitant organiser la gestion de la sécurisation de ses systèmes d'information et de ses échanges électroniques. Ainsi les institutions bancaires peuvent aussi recourir au RGS pour désigner les prestataires de service de confiance pour assurer la sécurité de l'ensemble de "documents transférables électroniques" avec leurs usagers, tels que les chèques, lettres de change ou billets à ordre, ainsi de leur aider à régir leur relation avec les prestataires.

721. Donc, dans le domaine de la sécurité des systèmes informatique, le RGS est considéré comme un guide général de bonnes pratiques conformes à l'état de l'art, mis à la disposition de tout organisme désirant recourir à des prestataires de confiance.

iii. Fonctions du RGS

722. Le référentiel détermine les règles qui régissent la disponibilité, l'intégrité et la confidentialité des données, en fonction du niveau de sécurité adopté par l'autorité administrative ou tout autre organisme souhaitant organiser la gestion de la sécurisation de ses systèmes d'information et de ses échanges électroniques.

723. Le RGS met en œuvre des mécanismes de cryptographie asymétrique en utilisant deux clés : une clé privée, permettant à l'émetteur de signer son message et une clé publique, qui permet au destinataire de le décrypter[331].

724. Comme le RGS présente pour l'ensemble des prestataires de services un guide de bonnes pratiques, il propose principalement 2 solutions :

- une méthodologie orientée autour de la responsabilisation des autorités vis-à-vis de leurs systèmes d'information à travers la démarche d'homologation ;

[331] Voir *Supra* n°795 s.

- des règles et bonnes pratiques que doivent mettre en œuvre les administrations ainsi que tout prestataire de service souhaitant recourir à des prestations spécifiques : certification et horodatage électroniques, audit de sécurité.

725. Quant à la valeur juridique des règles annoncées par le RGS, elles sont considérées comme des recommandations suivies dans le domaine de la sécurité des systèmes informatique et les échanges électroniques et fortement sollicitées par les usagers[332].

b) Référentiel général d'interopérabilité (RGI)

726. Il s'agit d'un référentiel qui est prévu également par l'ordonnance du 8 décembre 2005 dans son article 11, et adopté par l'arrêté du 9 novembre 2009. Le RGI dispose d'un cadre commun d'harmonisation, qui détermine les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il sert à déterminer notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les usagers.

727. En France, après une longue période d'attente, le gouvernement a publié au Journal officiel du vendredi 22 avril l'arrêté en date du 20 avril 2016 portant approbation de la nouvelle version du RGI[333]

728. La nouvelle version du RGI a apporté quelques modifications à l'ancienne version pour s'adapter aux nouvelles technologies informatiques. C'est un guide pratique qui prévoit des recommandations pratique qui prévoit des recommandations respectées par tous les usagers dans le domaine de sécurité informatique et interopérabilité, y inclus principalement « les autorités administratives » du pays. Le RGI a pour objet d'assurer l'interopérabilité[334] et la fonctionnalité entre les différents systèmes afin de faciliter et simplifier les échanges par voie électronique.

[332] Nous entendons ici par usagers l'ensemble des acteurs de l'achat de produits ou de prestations liés à la sécurité des systèmes d'information, y inclus les institutions financière pour protéger les "documents transférables électroniques".
[333] Arrêté du 20 avril 2016 portant approbation du référentiel général d'interopérabilité. [En ligne : https://www.legifrance.gouv.fr/eli/arrete/2016/4/20/PRMJ1526716A/jo/texte].
[334] Voir *supra* aussi n°1119.

729. L'interopérabilité joue dans le sens où il s'agit de prévenir, voire éviter qu'un document émis par un service ne puisse être lu sur l'ordinateur de son destinataire (c.-à-d. celui qui reçoit le document électronique et ayant le droit de s'en prévaloir et s'en servir).

730. Ainsi il faut veiller d'utiliser des formats uniformes. Citant à titre d'exemple la décision des autorités de privilégier le format ODF – qui se décline en « .odt », « .ods », « .odb »... La nouvelle version du RGI a placé ce format en « recommandé », tandis que l'OOXML de Microsoft (« .docx », « .xlsx »...) reste « *en observation* », notamment du fait de « *sa complexité* », et de « *son manque d'ouverture* ». La raison pour laquelle le RGI a conseillé l'usage du format ODF est sa simplicité et son interopérabilité sur différents systèmes.

Syntaxique	Document		
Recommandé	**ODF**	Open Document Format for Office Applications	
http://fr.wikipedia.org/wiki/OpenDocument OpenDocument est un format ouvert de données pour les applications bureautiques : traitements de texte, tableurs, présentations, diagrammes, dessins et base de données bureautique. OpenDocument est la désignation d'usage d'une norme dont l'appellation officielle est OASIS Open Document Format for Office Applications, également abrégée par le sigle ODF			
OASIS ISO	Open Document Format for Office Applications Version 1.2 ISO/IEC 26300-1:2015, ISO/IEC 26300-2:2015, ISO/IEC 26300-3:2015		

Syntaxique	Document		
En observation	**OOXML**	Office Open XML strict	
http://fr.wikipedia.org/wiki/Office_Open_XML Office Open XML est une norme ISO/CEI 29500 créée par Microsoft, destinée à répondre à la demande d'interopérabilité dans les environnements de bureautique. Ce format (dont les suffixes sont .docx, .xlsx, .pptx...) est utilisé à partir de Microsoft Office 2007, en remplacement des précédents formats Microsoft (reconnus à leurs suffixes tels que : .doc, .xls, .ppt), il est toutefois légèrement différent, pour ces versions d'office, de la norme ISO définitive, qui a tenu compte des remarques des membres de l'organisme normalisateur. Seule la suite Office à partir de la version 2013 est totalement compatible avec la norme (en lecture et en écriture). Le standard est conservé dans le RGI au statut « en observation ». Sa complexité, son manque d'ouverture (notamment dans la gouvernance de la norme) et le strict respect tardif de la norme par Microsoft même n'ont pas permis de réviser son statut. La version « *transitionnal* » de la norme n'est quant à elle pas recommandée. Pour des besoins d'échanges d'informations sous forme de tableaux qui notamment embarquerait du code, l'utilisation d'OOXML peut être une alternative. C'est toutefois une pratique à encadrer.			
ISO	ISO/CEI 29500 :2008-2012		

731. À l'instar du RGS, le RGI ne correspond nullement à des normes juridiques: il s'agit d'un ensemble de règles et normes techniques dont l'application est recommandée.

c) Référentiel général d'accessibilité des administrations (RGAA)

732. Etant adopté par le décret n° 2009-546 du 14 mai 2009 pris en application de la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des

chances[335], le RGAA vise à permettre à toute personne, quelle que soit la nature de son handicap, d'accéder aux contenus et services en ligne des administrations, et ainsi définit notamment les critères d'accessibilité des sites Internet.

733. Ce RGAA mérite simplement d'être mentionné dans ce document en tant que référentiel utilisée par les autorités administratives, bien qu'il n'a pas vraiment lieu dans notre étude des "documents transférables électroniques" car il n'est pas associé au rôle du prestataire de services de confiance, et il est temps de passer à l'étude des systèmes de certification.

B. Le système de certification

1) Notion de certification.

734. D'après l'ordonnance n° 2005-1516, art. 1er, II, 3e, les certificats électroniques sont délivrés par une tierce personne, qui est le *prestataire de services de confiance*.

735. Un certificat constitue un dispositif de vérification d'une signature électronique ; il est défini à l'article 3 (14)[336] du règlement du 23 juillet 2014 comme "*une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne*".

736. Pour obtenir un certificat qualifié de signature électronique, l'article 3-15[337] dudit règlement prévoit que le certificat est délivré par le prestataire de services de confiance qualifié et qui satisfait aux exigences visées à l'annexe 1[338].

---

[335] Loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées. *Journal Officiel 16 Mai 2009, version consolidée au 23 novembre 2016.* [En ligne : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000809647].

[336] Article 3 (14) du Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. [En ligne : http://data.europa.eu/eli/reg/2014/910/oj].

[337] Article 3 (15) du Règlement (UE) n ° 910/2014.

[338] L'Annexe I du Règlement (UE) n ° 910/2014 prévoit les exigences concernant les certificats qualifiés; tout certificat qualifié doit comporter:

737. La certification permet d'attester par une tierce partie indépendante et impartiale qu'un produit ou un document atteint, à un instant donné, un niveau de sécurité représenté par les services de sécurité qu'il offre et sa résistance à un niveau d'attaques donné : en France, quel que soit le type d'évaluation, la certification s'appuie systématiquement, outre des vérifications de conformité, sur des tests d'intrusion pour déterminer le niveau de sécurité réellement atteint par le produit ou le document électronique[339]

738. Ainsi la fonction du certificat électronique, délivré par un prestataire qualifié, garantit le lien entre l'identité du signataire et la clé publique, qui lui aura été présentée par porteur identifié. Le certificat électronique est constitué de trois composantes:

- des informations relatives à l'identité du titulaire (nom, prénom, fonction, service...) et à son organisation ;
- une clé privée ;
- une clé publique.

739. La certification permet de répondre aux objectifs réglementaires de l'union européenne, tels que l'application de directives européennes et nationales.

---

a) une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié de signature électronique;
b) un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins l'État membre dans lequel ce prestataire est établi, et
- pour une personne morale: le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels;
- pour une personne physique: le nom de la personne ;
c) au moins le nom du signataire ou un pseudonyme; si un pseudonyme est utilisé, cela est clairement indiqué;
d) des données de validation de la signature électronique qui correspondent aux données de création de la signature électronique;
e) des précisions sur le début et la fin de la période de validité du certificat;
f) le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié;
g) la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat;
h) l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé mentionnés au point g);
i) l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié ;
j) lorsque les données de création de la signature électronique associées aux données de validation de la signature électronique se trouvent dans un dispositif de création de signature électronique qualifié, une mention l'indiquant, au moins sous une forme adaptée au traitement automatisé.

[339] La certification de sécurité par l'ANSSI, document publié le 09 Septembre 2015, [En ligne : http://www.ssi.gouv.fr/uploads/2014/10/certification_fr.pdf].

2) Procédure de certification

740. Du point de vue procédural, l'obtention d'un certificat électronique suppose le dépôt, auprès d'une autorité d'enregistrement, d'un dossier comprenant la demande de certificat écrite signée et datée de moins de 3 mois par le futur porteur, un document officiel d'identité en cours de validité comportant une photographie d'identité, l'adresse postale et/ou l'adresse mail permettant à l'autorité de certification de contacter le porteur, les conditions générales d'utilisation signées.

741. La procédure de certification de la sécurité s'effectue principalement en deux étapes, sous la surveillance de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) :

- Evaluation de la sécurité du produit ou du système en vue de la certification.

742. La personne, appelée le commanditaire, intéressée par une certification d'un système de sécurité, devra déposer un dossier auprès de l'ANSSI[340].

743. Le dossier doit comporter le descriptif du système de sécurité faisant l'objet de l'évaluation, les dispositions lui conférant sa pleine efficacité et le programme de travail prévisionnel permettant son évaluation. Lors de l'évaluation par l'ANSSI, si l'agence estime que les objectifs de sécurité ne sont pas atteints, il notifie le commanditaire qu'elle ne pourra pas en l'état du dossier procéder à la certification envisagée.

744. Ce n'est qu'après un avis favorable à cette demande que le commanditaire puisse choisir un des centres d'évaluation agréés ; ce dernier remettra, à son tour, à l'ANSSI un rapport d'évaluation servant de base pour l'élaboration d'un rapport de certification.

745. Ensuite, le commanditaire et l'ANSSI vont valider les rapports d'évaluation en liaison avec le centre d'évaluation intervenant. Une fois tout est validé, l'ANSSI élabore un rapport de certification dans un délai d'un mois. Ce rapport

[340] D. 18 av. 2002, art. 2 s.

précisera les caractéristiques des objectifs de sécurité proposés, et conclut soit à la délivrance d'un certificat, soit au refus de la certification[341].

- La certification du système de sécurité.

746. Le certificat est délivré par le Premier ministre et *« atteste que l'exemplaire du produit et du système soumis à évaluation répond aux caractéristiques de sécurité spécifiés. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises »* [342].

747. De ce qui précède, nous retenons que le centre de certification de l'ANSSI est en charge d'étudier tout besoin de sécurité des multiples donneurs d'ordres. Il offre ces services de certification de manière gratuite et accessible à tout le monde.

748. Il est aussi important de signaler que le centre fait recours à des experts de l'ANSSI dans ces missions, et il s'appuie sur des laboratoires d'évaluation agréés (Centre d'Evaluation de la Sécurité des Technologies de l'Information). De leur côté, le centre prend compte de vérifier leurs compétences techniques sur les différents domaines techniques pour lesquels ils sont agréés, et valide la pertinence de leurs travaux pour chaque produit évalué.

749. D'ailleurs, le schéma français de certification offre deux types d'évaluation selon les besoins de sécurité exprimés par des commanditaires d'évaluation et des donneurs d'ordres[343].

- La Certification de Sécurité de Premier Niveau est une évaluation réalisée en temps contraint et donc sur des charges de travail fixées au préalable ; elle nécessite un investissement relativement limité, et est nettement plus orientée tests d'intrusion que conformité.

[341] Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, Version consolidée au 23 novembre 2016. Art. 7 et s. [En ligne : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005632663].
[342] *Op. Cit.* Art. 8 s.
[343] Service de certification auprès de l'ANSSI, [En ligne : http://www.ssi.gouv.fr/administration/produits-certifies/].

- L'évaluation selon les Critères Communs permet quant à elle de certifier un produit selon des niveaux d'assurance de sécurité *Evaluation Assurance Level* très variés, allant de EAL1 (niveau d'attaquant faible, *script kiddie*) à EAL7 (niveau d'attaquant élevé), et prend également en compte la sécurité du développement.

PARAGRAPHE II/ RÉGIME JURIDIQUE DES PRESTATAIRES DE SERVICES DE CONFIANCE

750. Les prestataires de services de confiance aujourd'hui disposent d'un cadre juridique uniforme pour régir leur qualification sur le marché européen ainsi que le domaine de leur intervention, et les services qu'ils offrent à leurs clients.

A. Statut juridique des services de confiance

1. Présentation du système juridique gouvernant les services de confiance en Europe

a) La reforme européenne en matière d'identification électronique et services de confiance

751. Au niveau européen, la première intervention du législateur européen était en 1999 lors de l'adoption de la directive n° 1999/93/CE ayant pour objectif de déterminer le régime juridique applicable aux signatures électroniques et aux activités des prestataires de service de certification[344].

752. Après 15 ans d'application et mise en épreuve de la directive de 1999, le législateur européen est revenu sur cette dernière en admettant que celle-ci était insuffisante, car elle ne dispose pas d'un cadre transfrontalier et intersectoriel complet pour des transactions électroniques sécurisées, fiables et aisées à utiliser[345].

[344] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, [En ligne : http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:31999L0093].

[345] D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », février 2015, [En ligne : https://www.droit-technologie.org/wp-content/uploads/2016/11/annexes/dossier/273-1.pdf].

753. Ainsi le législateur européen a abrogé la directive n° 1999/93/CE, par la mise en œuvre du règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS)[346]

754. L'objectif de ce Règlement consiste principalement à mettre en place un cadre juridique visant à susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur et d'instaurer un cadre juridique général concernant l'utilisation des services de confiance[347]. Le Règlement consiste aussi à renforcer la sécurité juridique, au profit tant des prestataires de services que des utilisateurs de ces services. Comme l'évoque d'ailleurs le premier considérant du Règlement, l'amélioration de la sécurité juridique devrait contribuer au renforcement du climat de confiance[348].

755. Ce Règlement abroge la directive de 1999, mais il en reprend néanmoins la plupart de ses dispositions, moyennant quelques modifications, et complète celles-ci par de nouvelles dispositions relatives, d'une part, à la reconnaissance mutuelle au niveau de l'Union européenne des schémas d'identification électronique notifiés et, d'autre part, aux services de confiance complémentaires à la signature électronique, telles que l'authentification de site web, l'horodatage ou le cachet électronique.

756. Ainsi, ce nouveau texte du règlement répond aux défis posés par le déploiement du numérique au sein du marché interne, et apporte une solution efficace au manque de confiance des utilisateurs dans les systèmes électroniques par rapport aux interactions physiques[349].

---

[346] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, *Journal officiel de l'Union européenne*, 28 aout 2014. [En ligne :http://data.europa.eu/eli/reg/2014/910/oj].

[347] Chapitre 3 du Règlement européen du 23 juillet 2014 consiste à instaurer un cadre juridique général concernant l'utilisation des services de confiance. Considérant n° 21 et article 1, b) et c).

[348] Considérant n°1 de la Règlement (UE) n ° 910/2014: « *Instaurer un climat de confiance dans l'environnement en ligne est essentiel au développement économique et social. En effet, si les consommateurs, les entreprises et les administrations n'ont pas confiance, notamment en raison d'un sentiment d'insécurité juridique, ils hésiteront à effectuer des transactions par voie électronique et à adopter de nouveaux services* » et considérant n° 14 : « *Le présent règlement vise à établir un cadre cohérent en vue de fournir des services de confiance d'un niveau de sécurité et de sécurité juridique élevé* ».

[349] PE et Cons. UE, prop. de règl. : Doc. COM (2012), 238 final, http://ec.europa.eu. – V.E.A. Caprioli et P. Agosti, *La régulation du marché européen de la confiance numérique : enjeux et perspectives de la proposition de règlement européen sur l'identification électronique et les services de confiance : Comm.com.electr.* févr. 2013, n 2, étude 3.

757. Le législateur européen a adopté la solution la plus cohérente en promulguant la Directive 1999/93 puis le Règlement n° 910/2014 dans une tentative d'unifier les règles de droit entre les Etats membre en matière de services de confiance.

b) Le label de confiance de l'Union pour les services de confiance qualifiés

758. Un "label" est aussi un autre outil pour fortifier la confiance des usagers. Celui ci est essentiel pour que les utilisateurs tirent pleinement avantage des services électroniques et qu'ils s'y fient en connaissance de cause.

759. L'article 23 du Règlement prévoit la création d'un label de confiance de l'Union qui permet d'identifier les services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés. De la sorte, ce label distinguerait clairement les services de confiance qualifiés des services de confiance non qualifiés, contribuant ainsi à la transparence du marché[350].

760. Suite à l'obtention par un prestataire du statut qualifié et qu'il soit inscrit sur la liste de confiance, il pourra utiliser le label de confiance de l'Union pour indiquer d'une manière simple, claire et reconnaissable les services de confiance qualifiés qu'il fournit (Article 23.1 du Règlement).

761. En plus, l'article 23, dans son alinéa 2, prévoit que le prestataire doit veiller à ce qu'un lien vers la liste de confiance concernée soit disponible sur son site Internet[351]. Cette liste est accessible au grand public et sert à tracer les services qualifiés.

762. L'utilisation des services qualifiés est non seulement fortement recommandée mais indispensable pour les 'documents transférables électroniques' en tant qu'effets de commerce électronique portant une valeur financière et qui circulent sur le web.

[350] Considérant n°47.
[351] Article 23.2 du Règlement (UE) du n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, Journal officiel de l'Union européenne, 28 aout 2014.

2. Les Conditions préalables à l'utilisation de services qualifiés

a) L'interopérabilité, un préalable à la reconnaissance mutuelle des Etats membres

763. Nous revenons ici sur la notion de l'interopérabilité pour évoquer l'importance de l'harmonisation des règles nationales pour gagner la confiance des utilisateurs sur l'utilisation des services qualifiés.

764. En matière de concordance et d'harmonisation entre les différentes législations nationales, et dans le but d'assurer une communication satisfaisante et la reconnaissance avec d'autres prestataires de service, il est important que l'interopérabilité des systèmes de signatures électroniques soit garantie, en respectant surtout les normes et les standards en vigueur.

765. D'après le considérant 54 du règlement *« L'interopérabilité et la reconnaissance transfrontalières des certificats qualifiés sont une condition préalable en vue de la reconnaissance transfrontalière des signatures électroniques qualifiées. Dès lors, les certificats qualifiés ne devraient faire l'objet d'aucune exigence allant au-delà des exigences énoncées dans le présent règlement. Cependant, il devrait être permis, au niveau national, d'inclure dans les certificats qualifiés des attributs spécifiques, tels que des identifiants uniques, pour autant que ces attributs spécifiques n'entravent pas l'interopérabilité et la reconnaissance transfrontalières des certificats et des signatures électroniques qualifiés.*

766. La Commission a constaté dans son analyse d'impact lors de la préparation de la proposition de règlement que « *le manque de confiance dans les systèmes électroniques, dans les outils fournis et dans le cadre juridique peut donner l'impression que les garanties juridiques sont moindres que dans le cas d'une interaction physique* »[352].

[352] Résumé de l'analyse d'impact accompagnant la proposition de règlement du 4 juin 2012 (SWD(2012) 136 final).
[En ligne : http://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX%3A52012SC0136].

767. Cette dernière déclaration par la Commission révèle que les principales causes de ce problème du manque de confiance et d'interopérabilité sont le fait que le cadre juridique en vigueur dans les Etats membres est insuffisamment développé ; nous ajoutons à cela le manque de coordination dans le développement et le contrôle des services offerts, le manque de transparence quant aux garanties de sécurité et le manque de sensibilisation des utilisateurs.

768. La création d'un cadre juridique uniforme, harmonisé, transparent sera en mesure de permettre à combler ces lacunes de sécurité et manque de confiance. Ainsi le Règlement de 2014 est parvenu à atteindre ses objectifs de sécurité en prévoyant des règles basées sur des mesures de sécurité d'un niveau élevé ainsi que la sensibilisation des utilisateurs pour les convaincre d'adhérer à ce projet commun devraient permettre de combler ces lacunes.

b) Procédure d'autorisation préalable et la demande de qualification.

769. Dans le cadre des échanges électroniques entre les usagers et les autorités administratives, tout prestataire de services de confiance peut demander à être qualifié. Cette qualification atteste de la conformité du service aux exigences du Référentiel Général de Sécurité (RGS) au niveau de sécurité requis. La qualification permet aussi au prestataire de demander à être référencé par l'Etat.

770. Les prestataires de services de confiance sont répartis en plusieurs familles. Nous avons par exemple les prestataires de services de certification électronique (PSCE) qui peuvent délivrer des certificats électroniques pour des usages tels que la signature électronique, l'authentification, le chiffrement. Il y a aussi les prestataires de services d'horodatage électronique (PSHE) qui délivrent des contremarques de temps pour un unique niveau de sécurité.

771. Pour être qualifié, le prestataire doit suivre la procédure d'autorisation préalable prévue à l'article 21 qui représente l'étape préliminaire avant de commencer à offrir des services de confiance qualifiés, contrairement à l'offre de services de confiance non qualifiés qui n'exige aucune autorisation, ni procédure ou formalité préalable.

772. D'abord, lorsqu'un prestataire prend l'initiative d'offrir un service de confiance qualifié, il doit concrétiser son initiative par soumettre à un organe de contrôle national une notification de son intention accompagnée d'un rapport sur l'évaluation de la conformité délivré par un organisme d'évaluation de la conformité[353].

773. Par la suite, l'ANSSI, désignée comme organe de contrôle les autorités françaises, prendra une décision de qualification d'un prestataire de services de confiance sur la base de ce rapport d'évaluation rendu par l'organe de contrôle.

774. Le prestataire de services de confiance doit obligatoirement attendre être déclaré « qualifié » afin de pouvoir démarrer leur activité en tant que prestataire de des services de confiance qualifiés. Son statut de « qualifié » sera indiqué sur une liste[354]. Ces listes nouvellement consacrées par l'article 22 du Règlement[355] sont d'une importance significative pour les prestataires de services de confiance, et conditionne l'utilisation des services qualifiés pour ces derniers[356].

775. Ces listes sont sécurisées et accessibles en ligne à tout moment, permettant ainsi à tout utilisateur de vérifier de manière fiable si un prestataire auquel il compte recourir est effectivement inscrit sur la liste et dispose du « statut qualifié ».

776. L'article 22 stipule d'ailleurs sur les listes de confiance que chaque Etat membre est tenu responsable pour établir, tenir à jour et publier, de façon

[353] Note de l'ANSSI sur « les Prestataires de services de confiance qualifiés – critères d'évaluation de la conformité au règlement eIDAS », Version 1 du 4 mai 2016. Page 5.
Selon l'article 3,18), un "organisme d'évaluation de la conformité" est un organisme défini à l'article 2, point 13), du règlement (CE) n° 765/2008 (du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, JO L 218 du 13.8.2008, p. 30), qui est accrédité conformément audit règlement comme étant compétent pour effectuer l'évaluation de la conformité d'un prestataire de services de confiance qualifié et des services de confiance qualifiés qu'il fournit.
[354] Cette affirmation découle d'une lecture *a contrario* de l'article 21.3.
[355] Article 22 du règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.
[356] En ce sens, le considérant n° 46 indique que « *Les listes de confiance sont des éléments essentiels pour fonder la confiance des opérateurs économiques, car elles indiquent le statut qualifié du prestataire de service au moment du contrôle* ».

sécurisée et sous une forme adaptée au traitement automatisé, les listes de confiance.

777. Il faut signaler que sous l'ancien régime, la directive 1999/93/CE se limitait à mettre en place un système de « déclaration » préalable par les prestataires qualifiés et l'éventualité de procéder à un contrôle à posteriori sans délai spécifique. Ceci s'explique que le système juridique permettait aux prestataires d'offrir leurs services dès la notification de leur demande et la remise du rapport d'audit, sans avoir besoin d'attendre la décision de l'autorité de contrôle qui pouvait leur être défavorable[357].

778. Désormais le Règlement 2014 adopte un système « d'autorisation » préalable. Par conséquent, un prestataire est tenu d'attendre la décision d'octroi du statut "qualifié" pour pouvoir exercer ses fonctions avec ce nouveau titre, et l'organe de contrôle ne dispose que de trois mois en principe pour examiner et valider la demande et statuer sur sa demande soit d'accorder ou non le statut « qualifié » au prestataire.

779. Le législateur se montre ainsi plus prudent et conscient de l'importance de l'obtention du statut « qualifié » pour un prestataire de services qualifiés afin de pouvoir se lancer sur le marché.

780. D'ailleurs, par extension du champ d'application du prestataire de service, l'intervention de l'autorité de contrôle ne se limite plus à contrôler les prestataires de signature électronique mais s'étend aux prestataires de tous les autres services de confiance (i.e. cachet, horodatage, envoi recommandé et authentification de site web).

[357] Dans ce sens, le considérant 10 de la directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999 prévoit que *"... afin de favoriser la fourniture à l'échelle communautaire de services de certification sur des réseaux ouverts, il y a lieu que les prestataires de service de certification soient libres d'offrir leurs services sans autorisation préalable; on entend par "autorisation préalable" non seulement toute autorisation à obtenir par le prestataire de service de certification au moyen d'une décision des autorités nationales avant d'être autorisé à fournir ses services de certification, mais aussi toute autre mesure" ayant le même effet*".

B. Système de responsabilité des prestataires de services de confiance.

781. Les obligations et responsabilités du prestataire de services de confiance diffèrent selon qu'ils offrent des services de confiance qualifiés ou non qualifiés.

1. Services « qualifiés » Vs. « non qualifiés »

a) Libre choix de services « qualifiés » ou « non qualifiés » par le prestataire de services

782. Le Règlement dispose de deux régimes de contrôle, l'un applicable aux services « qualifiés » et l'autre pour ceux « non qualifiés ». Ce système mis en place par le règlement peut être qualifié d'optionnel, puisqu'il ouvre le choix aux prestataires de services de confiance d'opter soit pour la fourniture des services qualifiés ou non qualifiés.

783. Dans ce sens, le considérant n° 35 du Règlement stipule que « *Tous les prestataires de services de confiance devraient être soumis aux exigences du présent règlement…* » tout en précisant que « *Toutefois, eu égard au type de services fournis par les prestataires de services de confiance, il y a lieu de faire une distinction, au niveau de ces exigences, entre, d'une part, les prestataires de services de confiance qualifiés et, d'autre part, les prestataires de services de confiance non qualifiés* ».

784. Pour utiliser une métaphore, le Règlement se limite à créer une « garde-robe » ou une « boîte à outils »[358] dans laquelle nous y trouvons deux « costumes juridiques » principaux : le costume juridique applicable aux services de confiance qualifiés et celui applicable aux services de confiance non qualifiés.

785. Le Règlement n'impose pas l'obligation aux acteurs économiques de choisir un de ces "costumes juridiques", voire "même les deux". Il n'impose pas d'ailleurs de porter toutes les pièces du costume : par exemple un prestataire

[358] D. GOBERT, *Supra* voir p.195, n°739.

pourrait offrir des services de signature et cachet électroniques, sans toutefois offrir des services d'horodatage et d'envoi recommandé électronique.

786. Bien que le règlement repose sur un système optionnel, lorsqu'un prestataire décide de fournir un ou plusieurs services de confiance, il sera obligé de se conformer aux critères du Règlement.

787. Ainsi le fait pour un prestataire de services de confiance de déclarer offrir des services de confiance « qualifiés » implique pour lui d'accepter implicitement de se soumettre aux exigences du Règlement relatives à cette catégorie de services.

788. Le Règlement consacre le concept de service de confiance «qualifié » dans son considérant n°28 en précisant que « *les notions de service de confiance qualifié et de prestataire de services de confiance qualifié devraient être introduites en vue de définir les exigences et obligations qui assurent un niveau élevé de sécurité de tous les services et produits de confiance qualifiés qui sont utilisés ou fournis* ».

789. Par souci de simplification, nous utilisons la métaphore suivante : le service de confiance non qualifié peut être comparé au modèle de base d'un véhicule « traditionnel » alors que le service de confiance qualifié s'apparenterait à un véhicule de grosse cylindrée, dotés de 4 roues motrices et de toutes les options.

790. Nous nous posons ici la question sur le choix du modèle par l'utilisateur, et la réponse dépendra certainement de la stratégie juridique et de la politique de gestion de risques de l'utilisateur.

791. Le premier choix réside pour un utilisateur qui utilise ces services dans un domaine dans lequel nous pouvons se satisfaire d'un niveau de sécurité et de fiabilité faible et/ou pour des opérations juridiques pour lesquelles le risque de contestation est faible voire acceptable.

792. Dans ce cas, l'utilisateur pourra se contenter d'un service non qualifié de la même manière qu'il n'est pas nécessaire de disposer d'un véhicule suréquipé pour rouler 20 km par jour sur des routes bien entretenues et sans obstacle.

793. Par contre, lorsque l'utilisateur se sert de ces services dans un domaine dans lequel un niveau de sécurité élevé est requis tant les risques d'attaques ou de fraudes sont importants et/ou pour des opérations juridiques pour lesquelles nous ne pouvons se permettre de prendre le risque d'une contestation tant les enjeux juridiques, économiques et financiers sont considérables, il adoptera un service de confiance qualifié. Par exemple en matière bancaire, les effets de commerce sont des instruments financiers qui risquent de fraude pendant leur exécution, ce qui nécessite une protection renforcée en faisant recours aux services de confiance qualifiés.

794. Dans ces dernières hypothèses, nous voyons l'importance pour l'utilisateur de recourir à un service de confiance qualifié de la même manière que s'il veut accéder au sommet d'une montagne en passant par un chemin semé d'embûches et de nombreux bourbiers, nous lui conseillerons d'utiliser un véhicule ad hoc lui permettant de franchir aisément ces obstacles en sécurité[359].

b) Les clauses de présomptions (ou d'assimilation) dans les services «qualifiés»

795. Tous les services de confiance qualifiés bénéficient d'une clause dite d'assimilation ou de présomptions ; cette clause dispensera son utilisateur de la charge de la preuve en cas de contestation, et le prestataire est présumé fautif jusqu'à preuve du contraire[360].

796. Au contraire, les services de confiance non qualifiés bénéficient simplement de la clause de non-discrimination ; cette clause consiste à considérer l'effet juridique et la recevabilité du service de confiance non qualifié comme preuve en justice, ne pouvant être refusés au seul motif que ce service se

[359] D. GOBERT, *Op. cit.*, p. 25.
[360] Dans ce sens, l'article 13 Règlement du 23 juillet 2014 prévoit que " Un prestataire de services de confiance qualifié est présumé avoir agi intentionnellement ou par négligence, à moins qu'il ne prouve que les dommages visés au premier alinéa ont été causés sans intention ni négligence de sa part".

présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du même service de confiance qualifié[361] (nous développons plus tard dans la présente section la responsabilité des prestataires de service de confiance[362])

797. Nous citerons quelques articles dans le texte du Règlement européen du 23 juillet 2014 pour illustrer la clause d'assimilation :

- l'article 25.2 prévoit que « *L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite* »,
- l'article 35.2. prévoit que « *Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié* »,
- l'article 41.2. prévoit que « *Un horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure* »,
- l'article 43.2. prévoit que « *Les données envoyées et reçues au moyen d'un service d'envoi recommandé électronique qualifié bénéficient d'une présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et à leur réception par le destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées par le service d'envoi recommandé électronique qualifié* ».

798. Nous saisissons de ces textes susmentionnés que lorsque le prestataire utilise un service qualifié, sa responsabilité devient plus élevée ; et en cas de litige soulevé entre les parties, le prestataire est présumé coupable jusqu'à ce qu'il apporte la preuve le libérant de sa responsabilité. Cette clause d'assimilation ou des présomptions de respect de garanties bénéficient aux services de confiance « qualifiés » mais pas aux services de confiance « simples ou non qualifiés ».

[361] Voir les articles 25.1., 35.1., 41.1. et 43.1 du Règlement européen du 23 juillet 2014.
[362] Voir n°825 s.

2. <u>Les engagements juridiques des prestataires de services de confiance qualifiés</u>

a) Obligations des prestataires de services de confiance qualifiés

799. La note publiée par l'ANSSI sur les Prestataires de services de confiance qualifiés et leurs critères d'évaluation de la conformité a traité juridiquement et techniquement en détail les obligations qui relèvent du prestataire de services qualifié.

800. Il nous suffit ici d'aborder les obligations juridiques prévues par le révérenciel de l'ANSSI selon l'ordre suivant.

i. Obligation de l'information et le compte rendu auprès de l'ANSSI.

801. La qualification du prestataire de services de confiance est délivrée pour une durée maximale de deux ans, conformément à l'article 20 du Règlement. Pourtant durant cette période, lorsqu'il y a des modifications considérables et jugées importantes dans la fourniture de ses services de confiance qualifiés, le prestataire de services de confiance a l'obligation d'informer l'ANSSI des modifications apportées aux services.

802. Il est aussi tenu d'adresser chaque année à l'ANSSI une synthèse de l'ensemble des modifications apportées à la fourniture de ses services de confiance qualifiés.

ii. Assurer la fiabilité des systèmes utilisés pour le stockage des données

803. Cette obligation était initialement prévue à l'annexe II de la directive du 13 décembre 1999, puis les mêmes dispositions étaient reprises à l'article 6 du décret du 30 mars 2001. Elle édictait que le prestataire de services de certification doit utiliser des systèmes et produits fiables tant pour leur fonctionnement que pour la conservation des certificats et employer du personnel qualifié.

804. Aujourd'hui depuis la publication de la note de l'ANSSI, le prestataire de services de confiance doit utiliser des systèmes fiables pour stocker les données

qui lui sont fournies, sous une forme vérifiable tout en respectant les conditions suivantes[363] :

- les données ne doivent pas être publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données ;
- seules des personnes autorisées peuvent introduire et modifier les données conservées ;
- l'authenticité de ces données peut être vérifiée.

iii. Rôle de « Risk Assessment » (Analyse de Risques)

805. D'après le texte de l'article 19 du Règlement, *les prestataires de services de confiance qualifiés et non qualifiés prennent les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent*.

806. Le prestataire de services de confiance joue ici le rôle de '*risk assessment*'. Il s'agit d'une obligation d'effectuer une analyse de risques sur le système d'information utilisé pour la gestion du service de confiance et procéder à son homologation.

807. Le périmètre de l'analyse de risques et d'homologation doit inclure le système d'information utilisé par le service de confiance et la protection des données à caractère personnel.

808. Cette analyse de risque et la décision d'homologation doivent être jointes au rapport d'évaluation de la conformité transmis lors de la demande de qualification.

[363] Section II.3.2 de la note de l'ANSSI sur « *les Prestataires de services de confiance qualifiés – critères d'évaluation de la conformité au règlement eIDAS* », version 1 du 4 mai 2016. Page 6, [En ligne : https://www.ssi.gouv.fr/uploads/2016/06/eidas-pscqualifies_v1.0_anssi.pdf].

iv. Gestion des incidents « Incident management »

809. En cas des incidents d'atteinte à la sécurité ou la perte de donnée, le prestataire de services de confiance doit notifier à l'ANSSI dans un délai maximal de vingt-quatre heures suite à la connaissance de cette atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées[364].

810. Afin de réaliser ce processus de notification, le prestataire de services de confiance doit remplir un formulaire mis en ligne sur le site de l'ANSSI.

v. Langue des documents utilisés par le prestataire de services de confiance.

811. Finalement, les documents publiés par le prestataire de services de confiance à destination du public concernant les conditions générales d'utilisation et les politiques relatives à la fourniture des services doivent être accessibles en français.

3. Régime de la révocation et la suspension des certificats qualifiés en cas d'atteinte à la sécurité

812. Au niveau des Etats, lorsqu'un Etat membre reconnait une atteinte du schéma d'identification électronique ou de l'authentification, affectant la fiabilité de l'authentification transfrontalière de ce schéma, il doit notifier, suspendre ou révoquer immédiatement cette authentification transfrontalière ou les éléments altérés en cause, et d'informer les autres Etats membres et la commission européenne[365].

i. La Révocation des certificats qualifiés.

813. Lorsqu'un prestataire de services de confiance décide de révoquer un certificat, il doit enregistrer cette révocation dans sa base de données relative aux

[364] Section II.3.4 paragraphe 7.9 de la Note de l'ANSSI sur « *les Prestataires de services de confiance qualifiés – critères d'évaluation de la conformité au règlement eIDAS* », version 1 du 4 mai 2016, p. 6. Voir aussi article 19, 2) du règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

[365] Article 10 du règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

certificats et publie le statut de révocation du certificat en temps utile, et en tout état de cause dans les vingt-quatre heures suivant la réception de la demande. Cette révocation devient effective immédiatement dès sa publication.[366]

814. Par la suite, le prestataire de services de confiance doit fournir à toute partie utilisatrice des informations sur la validité ou le statut de révocation du certificat qualifié qu'il a délivré. Ces informations seront disponibles à tout moment et au-delà de la période de validité du certificat, sous une forme automatisée qui est fiable, gratuite et efficace[367].

815. Il est prévu également à l'article 28 du règlement 2014 que « *si un certificat qualifié de signature électronique a été révoqué après la première activation, il perd sa validité à compter du moment de sa révocation et il ne peut en aucun cas recouvrer son statut antérieur* ». Or, l'effet de la révocation est définitif et irrévocable. Une fois la décision est prise de révoquer un certificat qualifié de signature, le prestataire ne peut plus revenir sur la décision.

ii. La suspension.

816. La suspension du certificat qualifié ne porte pas les mêmes effets qu'une révocation, et ses conséquences juridiques sont nettement moins grave que lorsque nous sommes dans l'hypothèse de la révocation. Le consi*dérant (53) du règlement 2014 précise que « la suspension de certificats qualifiés est, dans un certain nombre d'États membres, une pratique opérationnelle établie des prestataires de services de confiance qui est différente de la révocation et entraîne une perte temporaire de validité d'un certificat. La sécurité juridique impose que le statut de suspension d'un certificat soit toujours clairement indiqué. À cet effet, les prestataires de services de confiance devraient avoir la responsabilité de clairement indiquer le statut du certificat et, s'il est suspendu, la période précise de temps durant laquelle le certificat est suspendu ».*

[366] Article 24 § 3 du Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, [En ligne : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32014R0910].

[367] Article 24 § 4 du Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, [En ligne : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32014R0910].

817. Ainsi, à la différence de la révocation qui est définitive et irrémédiable, la suspension entraine une perte temporaire du certificat qualifié et que c'est au prestataire de services de confiance de préciser la période de suspension ; ce règlement ne devrait pas imposer aux prestataires de services de confiance ou aux États membres de recourir à la suspension, mais devrait prévoir des règles en matière de transparence, dans les cas où cette pratique est disponible.

b) Responsabilité du prestataire de services de confiance et la charge de la preuve

818. Tous les prestataires de services de confiance devraient être soumis aux exigences du présent règlement, notamment en matière de sécurité et de responsabilité, pour assurer une diligence appropriée, la transparence et la responsabilité quant à leurs activités et à leurs services. Toutefois, eu égard au type de services fournis par les prestataires de services de confiance, il y a lieu de faire une distinction, au niveau de ces exigences, entre, d'une part, les prestataires de services de confiance qualifiés et, d'autre part, les prestataires de services de confiance non qualifies (Considérant 35 du Règlement)

i. Principe de la responsabilité des prestataires de services de confiance

1) Présentation du système de l'Infrastructure de gestion des clés (IGC)[368] dont le prestataire de services de confiance faisait partie.

819. En réalité, les prestataires de service de confiance représentent l'autorité de certification (A.C.) et ils sont issus d'un système composite, lorsqu'ils se situent au cœur d'une Infrastructure de gestion de clés (IGC).

820. S'agissant d'une infrastructure comprenant plusieurs entités ; ces entités ont des fonctions et des responsabilités distinctes. Plusieurs métiers peuvent coexister à côté des utilisateurs des certificats : Autorité de certification (A.C.), Opérateur de certification et Autorité d'enregistrement (AE), Services de

[368] Guide pratique sur la dématérialisation des marchés publics - Version 2.0 de décembre 2012, 19 décembre 2012, [En ligne : http://www.marche-public.fr/contrats-publics/Dematerialisation-marches-publics-guide-dec-2012.htm].

publication (annuaire ou liste de révocation des certificats ou des autorités de certification reconnues).

821. L'IGC est ainsi constituée d'un ensemble de moyens techniques, humains, documentaires et contractuels mis à la disposition des utilisateurs pour assurer un environnement sécurisé aux échanges électroniques. La mise en œuvre d'une infrastructure de gestion de clés permet de s'assurer de la correspondance entre une clé publique figurant dans un certificat et un titulaire du certificat (celui qui signe à l'aide de la clé privée associée à la clé publique), ainsi que de fournir des services à valeur ajoutée pour les transactions électroniques. D'autres services comme l'horodatage, le cachet électronique, la gestion des preuves ou la confidentialité (chiffrement) peuvent également être fournis par le prestataire.

822. L'IGC permet alors de vérifier et d'assurer l'exactitude et l'intégrité des informations concernant le titulaire (du certificat), qui seraient réunies lors de leur collecte au moment de l'enregistrement et figurant dans le certificat.

823. Ces données sont particulièrement importantes lors l'identification de l'auteur d'un acte ou de son authentification. Ces infrastructures empruntent différentes formes techniques, allant du modèle interne d'IGC pour un intranet d'entreprise jusqu'au modèle externalisé sur l'internet fonctionnant en mode service (*SaaS*).

824. Il ressort ainsi de ce système que la confiance dépend de l'ensemble des composantes de l'I.G.C. dont les rôles et les responsabilités sont définis dans la politique de certification (PC) et les conventions. Néanmoins, en cas de préjudice, c'est l'A.C. (le Prestataire de services de confiance.) qui sera responsable vis à vis de ses clients et des personnes qui se fient à la signature électronique.

825. De la sorte, le prestataire de services de confiance ne pourra être libéré de ses responsabilités en soutenant qu'une autre entité est responsable (ex : l'A.E. pour la collecte des données relatives à l'enregistrement ou l'opérateur pour les services de certification). Il pourra toutefois engager la responsabilité de cette

dernière sur la base des engagements contractuels souscrits entre eux au sein de l'I.C.P.

2) La responsabilité des prestataires de services de confiance dans le Règlement.

826. En général, le régime de responsabilité joue dans le sens où tous les prestataires de services de confiance sont responsables des dommages causés à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le règlement. "*Afin de faciliter l'évaluation du risque financier que les prestataires de services de confiance pourraient devoir supporter ou qu'ils devraient couvrir au moyen d'une police d'assurance, le règlement les autorise à fixer des limites, sous certaines conditions, à l'utilisation des services qu'ils proposent et à ne pas être tenus pour responsables des dommages résultant de l'utilisation de services allant au-delà de ces limites. Les clients devraient être dûment informés à l'avance des limites fixées*". (Considérant 37 du Règlement)

827. Sur les questions qui relèvent de la responsabilité des prestataires de service de confiance, le texte du règlement a sensiblement évolué par rapport à celui de la proposition de règlement de la Commission[369].

828. La proposition de Règlement consacrait une présomption de responsabilité à la charge de tous les prestataires de service de confiance en cas de non-respect du Règlement. Par contre, le législateur européen, dans l'article 13 du Règlement, opère une distinction claire entre les prestataires qualifiés et non qualifiés.

- D'une part, s'il s'agit d'un prestataire de services de confiance *non qualifiés*, la charge de la preuve du comportement fautif du prestataire de service pèse sur la personne physique ou morale qui a subi les dommages. Il lui incombe donc de prouver que, intentionnellement ou par négligence, le prestataire a manqué à ses

[369] Proposition de Règlement du Parlement européen et du conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, Bruxelles, 4 juin 2012, article 9, p. 25, [En ligne : http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com%282012%290238_/com_com%282012%290238_fr.pdf].

obligations prévues par le Règlement et que le dommage est la conséquence de ce manquement.

- D'autre part, lorsqu'il s'agit d'un prestataire de services de confiance *qualifié*, la charge de la preuve de l'exécution non fautive de ses obligations pèse sur ce prestataire. En effet, *il est présumé responsable, à moins qu'il ne prouve que les dommages ont été causés sans intention ni négligence de sa part* (article 13 du Règlement).

829. Une telle contrainte éventuelle, et le risque qui en résulte si cette preuve (technique) n'est pas apportée à suffisance, peuvent être de nature à dissuader certains utilisateurs à recourir aux services de confiance non qualifiés. Cette distinction se justifie essentiellement par la volonté du législateur européen de ne pas faire peser un régime juridique trop lourd sur les prestataires non qualifiés, au risque de freiner le développement de cette catégorie de prestataires, d'autant que les services offerts par ces derniers ne bénéficient pas des « incitations » qui découlent des clauses d'assimilation ou des présomptions exposées plus haut[370].

830. Le règlement (article 24, 2-c)) [371] prévoit qu'en cas de litige, les prestataires de services auront également à faire la preuve qu'ils sont financièrement fiables, pour pouvoir fournir des services de confiance qualifiés.

831. Ainsi les prestataires de services doivent disposer des garanties financières suffisantes pour fonctionner en permettant l'indemnisation des utilisateurs autant que de besoin et notamment par le bais de souscription d'une police d'assurance appropriée.

832. Par rapport au respect des législations nationales en matière de responsabilité civile, selon l'article 13.3 du règlement, les règles de la responsabilité à l'encontre du prestataire de services de confiance « *s'appliquent conformément aux règles nationales en matière de responsabilité* ». Le considérant n°37 du règlement précise d'ailleurs que le « *règlement n'affecte donc*

[370] Voir *supra* n°795 s.

[371] Article 24 du Règlement, alinéa 2-c) prévoit que « *en ce qui concerne le risque de responsabilité pour dommages conformément à l'article 13, maintient des ressources financières suffisantes et/ou contracte une assurance responsabilité appropriée, conformément au droit national* »

pas ces règles nationales, par exemple celles relatives à la définition des dommages, au caractère intentionnel ou à la négligence, ou les règles procédurales applicables en la matière ».

833. De ces deux textes du règlement, nous saisissons l'intention du législateur européen de ne pas se mêler dans les affaires internes pour chaque Etat membre concernant les règles de la responsabilité civile. Il laisse ainsi à chaque Etat le soin d'aménager leur système de responsabilité.

834. Lorsque nous sommes en mesure de traiter la responsabilité du prestataire de services de confiance, il est important de citer un adage célèbre en droit civil français selon lequel « *Nul ne peut se constituer de preuve à lui-même* »[372]. Il s'agit d'un principe qui relève du bon sens, et qui est en lien avec l'article 1315 du Code civil[373] ; cette formule est normative, elle a, selon la jurisprudence et la doctrine française, valeur de principe général du droit des obligations.

835. Il est évident qu'un élément produit de manière unilatérale n'aura pas la même force probante qu'un élément objectif, et il appartient au juge d'apprécier la réalité des faits[374], comme l'a souligné la Cour de cassation en 2012 dans son rapport annuel : *« ...la preuve du fait juridique est libre, quelle que soit donc la personne dont elle émane … mais la force de conviction sera souverainement appréciée par le juge. »*.

836. En procédant ainsi, l'activité et le processus adopté par un prestataire de service devraient être vérifiables et contrôlable, quoi qu'il soit internalisé ou externalisé ; et comme le processus est complètement automatisé et la traçabilité des opérations techniquement assurées, il ne sera pas vraisemblable pour un prestataire de service internalisé de pouvoir agir sur les preuves à produire en justice.

---

[372] La rédaction de l'adage, telle que retenue ici, que l'on trouve notamment chez Pothier (références *in* Mouly-Guillemaud, « *La sentence "nul ne peut se constituer de preuve à soi-même", ou le droit des preuves à l'épreuve de l'unilatéralisme* », *RTD civ*. 2007, p. 253 et s., note 18).

[373] Article 1315 du Code civil, crée par la loi 1804-02-07 promulguée le 17 février 1804 prévoit que « *Celui qui réclame l'exécution d'une obligation doit la prouver. Réciproquement, celui qui se prétend libéré doit justifier le paiement ou le fait qui a produit l'extinction de son obligation* ».

[374] Cass civ 2ème, 6 mars 2014, 13-14295.

837. De tout ce qui précède, nous concluons que l'internalisation de tout ou partie des services de confiance par une partie peut apporter les mêmes garanties qu'une solution externalisée dès lors que la solution répondra aux critères d'impartialité, de pérennité, de fiabilité et d'audibilités.

ii. Dérogation à la règle et limitation contractuelle de la responsabilité des prestataires de services de confiance

838. Contrairement à la proposition de la Commission qui n'avait rien prévu sur ce point, l'article 13.2 du Règlement permet aux prestataires de services de confiance d'aménager contractuellement leur responsabilité. Ce texte prévoit que « *Lorsque les prestataires de services de confiance informent dûment leurs clients au préalable des limites qui existent à l'utilisation des services qu'ils fournissent et que ces limites peuvent être reconnues par des tiers, les prestataires de services de confiance ne peuvent être tenus responsables des dommages découlant de l'utilisation des services au-delà des limites indiquées* ».

839. Nous retenons de ce texte qu'afin de faciliter l'évaluation du risque financier que les prestataires de services de confiance pourraient devoir supporter ou qu'ils devraient couvrir au moyen d'une police d'assurance, le Règlement les autorise à fixer des limites, sous deux conditions, à l'utilisation des services qu'ils proposent.

840. Premièrement, les clients doivent être dûment informés à l'avance des limites fixées, ce qui suppose une définition contractuelle de ces limites[375]. Deuxièmement, ces limites doivent être reconnaissables par des tiers[376], par exemple par l'insertion d'une notice relative à ces limites dans les conditions applicables au service fourni ou par d'autres moyens reconnaissables[377].

841. Contrairement à la Directive[378], le Règlement n'exige plus que ces limites soient indiquées dans le certificat qualifié lui-même, ce qui est assez logique

[375] Exemple de clauses : « le tiers doit être désigné soit à l'aide d'outils contractuels permettant son identification, et ce de façon non potestative, ou alors nommément directement»

[376] Notamment par une partie utilisatrice, telle une partie qui vérifie une signature ou un cachet électronique ou encore un destinataire d'un envoi recommandé électronique par exemple.

[377] Considérant n°37.

[378] La directive de 1999/93 précise dans son article 6 § 3 que "*les Etats membres veillent à ce qu'un Prestataire de services de certification puisse indiquer, dans un certificat qualifié, les limites fixées à son*

puisque tous les services de confiance n'utilisent pas nécessairement un certificat. Ceci n'empêche pourtant pas un prestataire de services de confiance d'indiquer ces limites dans le certificat.

842. La pratique des limites présente le double avantage que celles-ci seront reconnaissables par des tiers et elles pourraient éventuellement bénéficier à l'utilisateur du service de confiance[379].

843. Revenant au texte de la directive abrogée qui utilisait le terme « discernable » deux fois pour exiger de la part de prestataire que les limites indiquées dans le certificat soient d'une clarté discernable pour l'utilisateur. Ce terme a laissé perplexe le juriste. Il signifie que les limites d'utilisation (ex : engageant l'entreprise à l'exclusion de son employé en son nom personnel) du certificat doivent être perçues de façon à éviter toute confusion. Le terme « discernable » n'a pas été repris dans le texte du Règlement pour rendre le sujet plus clair et non ambigu pour le juriste européen.

844. Ainsi, il suffira que l'attention de la personne qui reçoit un certificat et un message signé soit attirée par une indication selon laquelle l'utilisation du certificat est limitée, sans qu'il soit nécessaire que ce soit tout le contenu de cette limite lui-même qui soit affiché.

845. – Conclusion intermédiaire – Ainsi le prestataire de services de certification joue un rôle essentiel pour la vérification de la validité des documents électroniques et leur signature. Une autre activité de confiance aussi importante : celle de la prestation de service d'horodatage électronique.

---

utilisation, à condition que ces limites soient discernables par des tiers. Le Prestataire de services de certification ne doit pas être tenu responsable du préjudice résultant de l'usage abusif d'un certificat qualifié qui dépasse les limites fixées à son utilisation" et selon l'article 6 § 4 "*dans un certificat qualifié, la valeur limite des transactions pour lesquelles le certificat peut être utilisé, à condition que cette limite soit discernable par des tiers. Le Prestataire de services de certification n'est pas responsable des dommages qui résultent du dépassement de cette limite maximale*".

[379] Par exemple, lorsqu'une personne signe un document par voie électronique ou qui appose un cachet électronique ne devrait pas être tenues au-delà des limites indiquées dans le certificat, limites dont la partie utilisatrice est dûment informée par la consultation du certificat lors de la vérification de la signature ou du cachet.

PARAGRAPHE III LES PRESTATAIRES DE SERVICES D'HORODATAGE ÉLECTRONIQUE (PSHE)

846. **- La sécurisation des dates et l'"horodatage" -** Le procédé électronique pour l'apposition d'une date d'expédition ou de réception - ce procédé, habituellement nommé "horodatage" en termes techniques, est cité par les articles 1369-7 et 1369-8 du Code civil qui renvoient à deux textes d'application : le *décret n° 2011-434 du 20 avril 2011* relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat[380] et l'*arrêté du 20 avril 2011* relatif à la reconnaissance de la qualification des prestataires de services d'horodatage électronique et à l'accréditation des organismes qui procèdent à leur évaluation[381].

847. Selon les besoins, les systèmes d'information fonctionnent sur leur propre perception d'un "temps système" ou s'en remettent à un horodatage relevant d'une source de temps externe fiable, le droit présente la même problématique. Les actes juridiques de toutes sortes (et les faits juridiques) s'exécutent ou se déroulent à un instant déterminé pour lequel une extrême précision dans la datation peut présenter une importance relative. Au contraire, lorsque le moment est primordial et qu'un intérêt juridique le justifie, le droit fait appel à la notion de "date certaine". L'horodatage sécurisé du décret peut passer pour la version électronique de la date certaine du droit.

848. Nous présentons ainsi dans cette dernière partie de la section consacrée à l'horodatage électronique la notion adoptée par le Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014, ainsi que les exigences pour satisfaire à la présomption de fiabilité (I), puis la qualification des services d'horodatage (II) et finalement de traiter le cadre juridique et la charge de la preuve (III).

[380] Décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat, *JORF* n°0094 du 21 avril 2011 page 7093.
[381] Arrêté du 20 avril 2011 relatif à la reconnaissance de la qualification des prestataires de services d'horodatage électronique et à l'accréditation des organismes qui procèdent à leur évaluation, *JORF* n°0094 du 21 avril 2011 page 7094.

I. Notion des services d'horodatages électroniques.

849. D'après le règlement (UE) n° 910/2014, l'horodatage électronique est défini comme « *des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant* ».

850. Un horodatage électronique qualifié doit satisfaire aux exigences fixées à l'article 42 du Règlement; il doit avoir comme fonction de :

a) *lier la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données;*
b) *être fondé sur une horloge exacte liée au temps universel coordonné; et*
c) *être signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente.*

851. La commission européenne a le devoir de fixer les normes à suivre pour pouvoir établir le lien entre la date et l'heure et les données, et les horloges exactes. Ce lien est présumé satisfait aux exigences du Règlement lorsqu'ils respectent les normes fixées par la commission à travers les actes d'exécution (*art. 42 paragraphe 2*).

852. Le lien entre la date et l'heure et les données est établi au moyen d'un module d'horodatage composé d'une application d'horodatage et d'un module cryptographique. Nous envisageons ici deux hypothèses définies dans le document publié par l'ANSSI sur les Services d'horodatage électronique qualifiés et les critères d'évaluation de la conformité au Règlement eIDAS[382] :

- Si l'application d'horodatage est embarquée dans le module cryptographique, alors l'application d'horodatage doit avoir fait l'objet au minimum d'une Certification de Sécurité de Premier Niveau (CSPN) selon une cible de sécurité vérifiée par l'ANSSI. Il est recommandé que l'application d'horodatage ait fait

[382] Services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS, version 1.0 du 4 mai 2016. [En ligne : https://www.ssi.gouv.fr/uploads/2016/06/eidas-horodatagequalifie_v1.0_anssi.pdf].

l'objet d'une certification selon les critères communs selon le profil de protection

- Si l'application d'horodatage n'est pas embarquée dans le module cryptographique (par exemple, l'application d'horodatage fonctionne sur un serveur lui-même connecté au module cryptographique), alors le PSHE doit démontrer la mise en place de mesures techniques et organisationnelles permettant de réduire les risques pesant sur le module d'horodatage. Il est recommandé que l'application d'horodatage ait fait l'objet d'une Certification de Sécurité de Premier Niveau (CSPN) selon une cible de sécurité vérifiée par l'ANSSI.

II. Qualification des services d'horodatages électroniques.

853. Le processus de qualification d'un service d'horodatage électronique ressemble celui du prestataire de services de confiance. La durée de qualification est limitée à 2 ans conformément à l'article 20 du règlement.

854. Le principe de transition de la qualification [RGS] vers [eIDAS] d'un service d'horodatage électronique est décrit à la section I.5 de la note sur les services d'horodatage électronique qualifiés et leurs modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS[383].

855. Un service d'horodatage électronique qualifié [RGS] peut prétendre à la qualification du règlement [eIDAS] sous les conditions suivantes :

1. Le service d'horodatage doit s'assurer que l'ensemble des rapports d'évaluation sur la base desquels la décision de qualification [RGS] du service d'horodatage électronique a été prononcée par l'organisme de qualification soit transmis à l'ANSSI ;

[383] Services d'horodatage électronique qualifiés - Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS, version 1.0 du 19 février 2016. [En ligne : https://www.ssi.gouv.fr/uploads/2016/06/eidas-horodatage-transition-rgs_v1.0_anssi.pdf].

2. Les rapports d'évaluation doivent permettre de s'assurer du respect des exigences du règlement [eIDAS] non couvertes par le [RGS][384], à savoir les procédures mises en œuvre par le PSHE afin de :

- prévenir l'ANSSI sous 24h en cas d'atteinte à la sécurité ou perte d'intégrité du service qualifié;
- prévenir l'ANSSI en cas de changement ou de cessation d'activité;
- maintenir les ressources financières suffisantes et/ou contracter une assurance responsabilité appropriée pour couvrir tout dommage dont il serait responsable.

856. Les services d'horodatage électronique qualifiés doivent respecter ces exigences supplémentaires [eIDAS] précitées (spécifiées au chapitre II) ; la conformité à l'ensemble ces exigences est évaluée par un organisme d'évaluation respectant les critères de reconnaissance des organismes d'évaluation de la conformité des prestataires de service de confiance, sachant que cet organisme d'évaluation peut être différent de celui qui a octroyé la qualification [RGS].

III. Le cadre juridique et la reconnaissance des services d'horodatages électroniques.

857. Le *décret du 20 avril 2011* définit les contraintes techniques applicables au procédé technique, puis les détails de la procédure administrative permettant de faire constater la conformité réglementaire et en conséquence, la "fiabilité du procédé".

858. En effet, la résolution du problème de sécurisation des dates en matière de documents électroniques est posée par l'article 1369-8 du Code civil français[385] qui se prononce pour la recherche de la fiabilité du procédé. Il prévoit que « *Lorsque l'apposition de la date d'expédition ou de réception résulte d'un procédé électronique, la fiabilité de celui-ci est présumée, jusqu'à preuve*

[384] Ces exigences supplémentaires [eIDAS] sont définies au chapitre II de la note sur les « Services d'horodatage électronique qualifiés - Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS », Version 1.0 du 19 février 2016, *Ibid.*

[385] Article 1369-8 du Code Civil, version consolidée au 10 août 2016 [En ligne : https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006438628].

contraire, s'il satisfait à des exigences fixées par un décret en Conseil d'Etat. Un avis de réception peut être adressé à l'expéditeur par voie électronique ou par tout autre dispositif lui permettant de le conserve ».

859. La technique ne pouvant pas garantir à 100 % la fiabilité du procédé, le droit s'en tire avec la création d'une "présomption". Cette parade est déjà employée dans l'*article 1316-4* du Code civil à propos de la signature électronique.

860. Cette présomption de fiabilité est consacrée dans deux textes juridiques, l'un d'ordre réglementaire et national et l'autre d'ordre législatif et communautaire :

861. - Le *décret du 20 avril 2011* est le premier texte juridique en France qui reconnait cette présomption de fiabilité pour les services d'horodatage ; l'article 2 du décret prévoit qu'*un procédé d'horodatage électronique est présumé fiable si le prestataire de services d'horodatage électronique mettant en œuvre ce procédé et le module d'horodatage utilisé satisfont aux exigences fixées dans le texte*. Ces exigences de la loi pour reconnaitre les services d'horodatage sont fixées à l'article 3 du décret[386].

[386] Article 3 du Décret n° 2011-434 du 20 avril 2011 prévoit que « Le prestataire de services d'horodatage électronique se conforme aux exigences suivantes :1° Disposer de personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services d'horodatage électronique ; 2° Appliquer des procédures de sécurité appropriées ; 3° Utiliser des systèmes et des produits assurant la sécurité technique et cryptographique des fonctions qu'ils assurent, notamment un module d'horodatage satisfaisant aux exigences de l'article 4 ; 4° Assurer que l'horloge interne du module d'horodatage est synchronisée avec une ou plusieurs sources de temps fiable selon les performances garanties par le prestataire de services d'horodatage électronique et cesser de délivrer des contremarques de temps en cas de désynchronisation en dehors des performances garanties ; 5° Prendre toute disposition propre à prévenir la falsification des contremarques de temps ; 6° Disposer d'un certificat d'horodatage ; 7° Conserver toutes les informations relatives au fonctionnement du service d'horodatage électronique et utiles à la manifestation de la preuve d'une date selon des règles appropriées de confidentialité et d'intégrité ; 8° Mettre à disposition des utilisateurs et des abonnés par les moyens les plus appropriés les informations suivantes : a) Ses coordonnées permettant d'entrer en contact rapidement et de communiquer directement avec lui ; b) Les conditions générales d'utilisation des services d'horodatage électronique ; c) Les conditions générales de vérification des contremarques de temps et notamment le certificat d'horodatage ; d) Les performances garanties et notamment la précision de la date des contremarques de temps et l'échelle de temps utilisée ; e) Les principales caractéristiques techniques des dispositifs utilisés et les procédures qu'il met en place ; f) Le cas échéant la mention de la qualification visée à l'article 6 ; g) Les voies ouvertes pour les réclamations et le règlement des litiges ; 9° Avoir défini un plan de cessation d'activité permettant de garantir la continuité du service de vérification des contremarques de temps émises ; en particulier, en cas de cessation d'activité le prestataire de services d'horodatage électronique doit informer préalablement les utilisateurs de cette cessation et des conditions dans lesquelles sera assurée la continuité du service de vérification des

862. De même pour la signature, la présomption de fiabilité du procédé permet de prétendre à la plénitude des effets juridiques de la signature électronique.

863. En outre, les utilisateurs qui souhaiteraient sécuriser d'avantage leurs documents électroniques en matière de date certaine peuvent recourir, si cela n'existe pas dans leur plate-forme de dématérialisation, à un service d'horodatage sécurisé ou à un prestataire spécialisé dit "tiers horodateur".

864. L'autre texte législatif à reconnaitre la présomption de fiabilité est le *Règlement (UE) n° 910/2014* qui a stipulé parmi ses objectifs d'instaurer un cadre juridique pour les services d'horodatages électroniques (article 1er).

865. Dans ce sens, le considérant 62 du Règlement de 2014 prévoit que « *Afin d'assurer la sécurité des horodatages électroniques qualifiés, le présent règlement devrait imposer l'utilisation d'un cachet électronique avancé, d'une signature électronique avancée ou d'autres méthodes équivalentes. Il est à prévoir que l'innovation pourrait déboucher sur de nouvelles technologies susceptibles d'assurer un niveau de sécurité équivalent pour les horodatages. En cas de recours à une méthode autre que le cachet électronique avancé ou la signature électronique avancée, il devrait revenir au prestataire de services de confiance qualifié de démontrer, dans le rapport d'évaluation de la conformité, que ladite méthode assure un niveau de sécurité équivalent et satisfait aux obligations énoncées dans le présent règlement* » .

866. Comme le cachet électronique qualifié et la signature électronique, l'horodatage électronique bénéficient d'une clause d'assimilation ou de présomption ; les horodatages électroniques ne peuvent pas être contestés du seul fait de leur forme électronique, parce qu'ils sont présumés équivalent à l'horodatage sous forme écrite. Cela aussi signifie que la recevabilité de l'horodatage comme preuve en justice ne pourra pas être refusé au seul motif que cet horodatage est présenté sous une forme électronique (*art. 41, 1e*).

---

contremarques de temps ; 10° Publier sans délai tout événement affectant la fiabilité des contremarques de temps émises ; 11° Etre capable de démontrer le respect des exigences précitées.

867. En cas d'apparition d'un litige, la charge de la preuve incombe sur le prestataire de services d'horodatage (PSHE) dans le sens où ce dernier est présumé fautif jusqu'à ce qu'il apporte la preuve le libérant de sa responsabilité. Pour la charge de la preuve que Le PSHE doit conserver pendant une durée minimale de sept ans après l'expiration de chaque jeton d'horodatage toutes les informations pertinentes concernant les données délivrées et reçues, notamment à fin de pouvoir fournir des preuves en justice[387].

868. Quant à la reconnaissance de l'horodatage électronique au niveau des Etats membres, lorsque l'horodatage électronique est qualifié, il bénéficie automatiquement d'une présomption d'exactitude de la date et de l'heure qu'il indique, et une présomption d'intégrité des données auxquelles se rapportent cette date et cette heure (*art. 41, 2e*).

869. Ainsi la reconnaissance d'un horodatage électronique qualifié délivré dans un État membre s'étend à l'ensemble des États membres (*art. 41, 3e*) c.à.d. que lorsqu'un État membre reconnait un horodatage électronique qualifié dans son territoire, les autres États membres sont tenus d'accepter et reconnaitre cet horodatage électronique qualifié dans leur territoire.

870. **– Conclusion intermédiaire** – Ayant traité les phases de création et de validation des 'documents transférables électronique', il est temps d'examiner l'exécution des documents dans l'environnement informatique.

[387] Cette obligation de conservation des données pour une durée minimum de sept ans est prévue à la section II.3.3 du document « Services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS », version 1.0 du 4 mai 2016. *Ibid.*

CONCLUSION DU CHAPITRE II

871. La signature électronique, en tant que support, est une exigence législative pour l'exécution du 'document transférable électronique', aidant à leur identification/authentification. La signature électronique détient désormais une présomption de fiabilité en matière de preuve.

872. Pour sécuriser le décryptage d'une signature électronique, nous disposons du mécanisme de la cryptologie à clé publique, selon lequel des clés asymétriques sont utilisées pour le chiffrement et le déchiffrement d'un document électronique. Ce système est jugé fiable par les utilisateurs et les techniciens.

873. Enfin les outils technologiques de la gestion des données évoluent avec le temps, et les entreprises peuvent aujourd'hui se servir de ces derniers pour développer leur activité, tel le *bigdata*.

874. L'émergence de l'externalisation des prestations informatiques, représentée principalement par le service *Cloud computing*, connaît un succès fulgurant au niveau mondial ; les prestataires de services informatiques misent sur les services Cloud pour conquérir le marché, en se servant de la technologie de la virtualisation et la mutualisation des ressources.

875. Tous ces services de gestion et de prestation de service informatique sont fournis par un des prestataires de confiance. Un 'document transférable électronique' doit être pris en charge par un prestataire de services qualifié au fin de la signature électronique et la fiabilité du 'document transférable électronique'.

CONCLUSION

DE LA PREMIÈRE PARTIE

876. Internet, phénomène inhérent au développement du commerce électronique et des technologies de l'informatique et de la communication (transcription de *l'anglais information and communication technologies*, ICT), doit être traité à la fois comme un terrain libre, à la disposition des usagers, et comme un terrain où des contraintes existent ; elles permettent une protection contre le piratage électronique et la diffusion non autorisée et illégale des données personnelles.

877. Aujourd'hui le règlement du 27 avril 2016 assure cette protection des données à caractère personnel et de la vie privée en matière informatique. Ce règlement relève le défi de maintenir l'équilibre entre d'un côté, la liberté de l'internet et la communication par voie électronique, et de l'autre côté la protection des données à caractère personnel.

878. Les 'documents transférables électroniques', qu'ils soient des instruments de mobilisation de créance ou garantie de créance, sont reconnus aujourd'hui et détiennent la même force probante que leur équivalent sous forme papier, et sont acceptables comme moyens de preuve devant le juge, dans la mesure où ils respectent les conditions nécessaires à leur validité et leur fiabilité.

879. La validité et la fiabilité des 'documents transférables électroniques' passent par la garantie de la signature électronique ; celle-ci étant généralement le fait de prestataire de services qualifié externe à l'entreprise.

DEUXIEME PARTIE

L'EXÉCUTION DU 'DOCUMENT TRANSFÉRABLE ÉLECTRONIQUE' DANS L'ENVIRONNEMENT INFORMATIQUE

880. Le ‘document transférable électronique’ a créé un défi quant à son utilisation dans un environnement informatique. L’exécution des moyens de paiement électroniques fait suite à leur cycle de vie ; cette phase est tout aussi importante que celle de leur création et leur validation via la signature électronique et les mécanismes de cryptologie.

881. Lors de l’exécution du ‘document transférable électronique’, nous devons nous conformer aux exigences classiques attachées au document papier. Ces exigences doivent être respectées pour maintenir la confiance des usagers. Elles sont de deux ordres.

882. D’une part, l’exigence d’unicité qui permet à un document papier de se présenter comme unique et quasiment irréprochable. Cette notion d’unicité sera abordée dans l’environnement informatique afin d’obtenir son équivalence pour les ‘documents transférables électroniques’, et par la suite designer un exemplaire faisant foi (**Chapitre 1**).

883. D’autre part, l’exigence de possession, notion classique en droit des biens, ayant pour éléments constitutifs le *corpus* et l’*animus*, caractérise l’exercice d’un droit dans l’univers papier. Il est nécessaire de lui trouver un substitut adéquat pour les ‘documents transférables électroniques’, puisque c’est grâce à la possession que le titulaire du document pourra prouver sa qualité et sa légitimité.

884. En dernier lieu, nous envisageons la conservation des documents électroniques en tant qu’une phase finale dans leur cycle de vie. Leur conservation est impérative afin de permettre la preuve des droits de chacun, dans l’hypothèse d’un litige. (**Chapitre 2**).

885. Il est important de signaler que les exigences susmentionnées ne distinguent pas entre les différents moyens de paiement, tels qu’une lettre de change, un billet à ordre ou un récépissé d'entrepôt. Ces instruments financiers sont traités sur un pied d'égalité en tant que documents électroniques. Pour cela, lorsque nous citons les documents électroniques dans cette deuxième partie, nous nous référons automatiquement aux moyens de paiement présentés dans la première partie.

CHAPITRE 1

ÉQUIVALENCE FONCTIONNELLE DE L' « UNICITÉ »

(UNICITÉ ET SINGULARITÉ D'UN 'DOCUMENT TRANSFÉRABLE ÉLECTRONIQUE')

886. Comme nous l'avons déjà dit, le numérique a envahi depuis les années 90 notre univers et notre quotidien au travers du développement des réseaux internet. Il faut admettre que la production numérique dépasse largement la capacité cérébrale d'un être humain puisqu'elle se compte désormais en exa-octets[388] soit 10 octets.

887. Les instruments financiers sont bien évidemment impactés par ces bouleversements fondamentaux dans un contexte d'échanges accrus incités par le développement des réseaux internet avec des conséquences immédiates sur les échanges entre les institutions financières et les usagers.

888. Ces échanges entrainent une automatisation des processus s'accompagnant d'un besoin de sécurité informatique fort ainsi qu'une dématérialisation de l'information ; ceci se fait par production native électronique via des flux de données électroniques entre acteurs qui abandonnent progressivement la numérisation à partir d'un original papier.

889. Bien que nous ayons abordé la question de la signature électronique dans la première partie, nous partons de l'hypothèse selon laquelle les documents électroniques – portant même des signatures "qualifiées" ou "sécurisées" – peuvent ne pas posséder intrinsèquement la caractéristique d'unicité lorsqu'ils sont utilisés avec la plupart des technologies actuelles.

890. Bien qu'une telle supposition nous paraisse invraisemblable, cela nous mène à penser que les documents électroniques peuvent pour la plupart être copiés sans que nous puissions aisément distinguer la "copie" de l'"original".

891. Pour y remédier ou pour sécuriser d'avantage l'usage des documents électroniques, plusieurs approches visant à créer l'équivalence fonctionnelle électronique d'un document papier unique pourraient être proposées et mises en œuvre.

[388] Exa-octet est un terme *informatique* qui signifie une unité de mesure de quantité d'information numérique, valant 10^{18} octets, et dont le symbole est *Eo*.

892. Ainsi, traitons dans un premier temps la notion de l'unicité technique du document électronique, pour pouvoir l'identifier et garantir sa singularité dans un environnement informatique (*section 1 : l'unicité technique des documents électroniques*).

893. Dans un deuxième temps, nous envisageons la possibilité de la désignation d'un exemplaire faisant foi afin de répondre aux préoccupations concernant l'unicité et l'intégrité du document électronique (*section 2 : désignation d'un exemplaire faisant foi*).

SECTION 1 - L'UNICITÉ TECHNIQUE DES DOCUMENTS ELECTRONIQUES

894. Nous présentons d'abord les termes connexes à l'unicité comme composants essentiels de la confiance numérique (Paragraphe I), pour pouvoir introduire la notion de l'unicité (Paragraphe II).

PARAPRAPHE 1 – L'INTÉGRITÉ, UN CRITÈRE ESSENTIEL POUR INSTAURER LA CONFIANCE NUMÉRIQUE.

Débat terminologique et termes connexes : « unicité », « intégrité » et « fiabilité »

895. Les termes ''intégrité' et 'fiabilité' présentent un enjeu capital pour les entreprises et tout usager des documents électroniques, tels que les chèques, les lettres de change ou billets à ordre. Il s'agit de minimiser leur risque juridique en cas de recours devant un tribunal, en s'assurant que leurs documents ne seront pas contestés devant le juge. Préserver l'intégrité et la fiabilité d'un document électronique nécessite pouvoir démontrer qu'il n'a pas été corrompu, de manière volontaire ou involontaire.

896. Nous évoquerons d'abord l'absence de normes législatives internationales uniformes. Il n'existe toujours pas de cadre juridique uniforme attribué aux

documents électroniques que nous pourrions considérer comme harmonieux, généralisé et accepté internationalement, pour traiter les différentes questions qui soulèvent de l'utilisation des instruments ou de documents titres transférables, et particulièrement l'utilisation de leur équivalent électronique, voire les 'documents transférables électroniques'.

897. Cette absence d'uniformité législative nous amène à nous interroger sur la notion de l'unicité technique : comment avoir un document électronique incontestable dans son intégrité et sa singularité alors même que les législations ne sont pas uniformes ?.

898. Dans le Code civil, le législateur français a introduit le terme « intégrité » dans le texte de l'article 1316-1[389] pour caractériser l'unicité de l'acte juridique passé sous forme électronique. Ce terme a entamé un grand débat sur l'usage de cette expression. Certains auraient préféré retenir le terme de « fiabilité »[390]. Leur raisonnement était fondé sur le fait que la jurisprudence liait depuis de longues années la preuve sur support électronique à la fiabilité des systèmes et logiciels utilisés lors de la création du document électronique en question.

899. La fiabilité est la confiance que nous accordions à un document électronique en tant qu'énoncé de faits ou contenu. La fiabilité est la responsabilité de l'auteur des documents, qu'il soit un individu ou une personne morale au nom de laquelle un individu rédige les documents. Cette fiabilité est évaluée en fonction de la complétude et de l'exactitude des documents, et du degré de contrôle exercé dans le cadre de son processus de création[391].

900. Ce terme 'fiabilité' se confond avec un terme similaire qui est l'"exactitude". Nous entendons par " exactitude " le fait que les données d'un document sont précises, justes, conformes à la vérité et exemptes d'erreurs ou de

[389] Article 1316-1 du Code civil prévoit que « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ». Code civil, version consolidée au 18 février 2015.
[390] M. Vivant, *Un projet de loi sur la preuve pour la société de l'information*, *Cahier Lamy droit de l'Informatique, Bulletin d'actualité*, 1999, Fascicule E, n°117, p.9.
[391] Alain Plantey et Marie-Cécile Plantey, *Fasc. 111 : Prescription Quadriennale – Domaine, maniement, effets, contentieux*, *LexisNexis* 16 Juillet 2014, n°17. Voir aussi : M. Vivant, *Op. cit.*, p.9 et s.

distorsion. Pour assurer l'exactitude d'un document électronique, il faut exercer un contrôle sur les processus de création, de transmission, de maintenance et de préservation des documents.

901. En fait, le législateur français a renoncé à l'usage du terme « fiabilité » longuement accepté par la jurisprudence française pour se montrer en faveur du terme « intégrité » attribué dorénavant aux documents électroniques.

902. D'après le législateur français, l'intégrité sert la complétude et la cohérence du document[392]. S'il apparait plus facile de vérifier la complétude et la cohérence d'un document papier, il en va autrement des documents électroniques plus compliqués dont les éléments constituants se séparent ; qu'il est primordial d'assurer, malgré la difficulté, leur intégrité pour préserver leur authenticité et maintenir la confiance à leur égard sur le marché.

903. Un autre argument en faveur de l'usage du terme 'intégrité' est que le critère de « fiabilité », lorsqu'il est évoqué, ne s'applique que pour les systèmes et aux procédés techniques engendrant la production de l'écrit, alors que le législateur français vise particulièrement l'écrit, plus que les procédés.

904. Aussi il ressort de l'analyse du terme « fiabilité » que nous avons du mal à constater l'existence de la fiabilité. Le juge français le considère une notion ambigüe et sujette à une appréciation au cas par cas. *En ce sens, retenir le terme de fiabilité aurait créé des risques de divergences d'appréciation. Au contraire, le terme d' « intégrité » vise spécifiquement l'écrit et constitue un état de fait objectif et réel. En conséquence, l'emploi du terme « intégrité » parait plus justifié que celui de « fiabilité »*[393].

[392] Charles KECSKEMETI et Lajos KORMENDY, *Les écrits s'envolent – La Problématique de la Conservation des Archives Papier et Numériques, Edition Favre SA* 2014.
[393] JOLY-PASSANT Elisabeth, *Op, cit.*, p. 380. n° 847. Voir aussi P. Gaudrat, *Introduction, in Une Société sans papier ? Droit de la preuve et nouvelles technologies de l'information (rapport-cadre), La documentation Française*, 1990, n°858, p. 385.

905. D'ailleurs, la littérature spécialisée n'est pas unanime au sujet de l'intégrité du document électronique. Plusieurs auteurs rattachent l'intégrité à la fixité[394]. La fixité est définie comme la « *qualité d'un document d'archives qui garantit une forme fixe et un contenu stable* »[395]. Nous trouvons que ce rattachement est peu judicieux. D'une part, le critère de fixité exige que l'aspect du document électronique ne change en rien, et pour ce faire, il faudrait conserver le logiciel originel et, d'autre part, la condition est inapplicable aux documents dynamiques qui changent constamment[396]. Pourtant, l'intégrité ne signifie pas que les fichiers et les métadonnées demeurent intactes car en réalité une telle stabilité espérée ne pourrait pas être atteinte.

906. Il est beaucoup plus judicieux de considérer l'intégrité comme une complétude conservant tous les éléments essentiels du document. Certes, le support d'un document électronique, disque dur ou CD, peut changer, la forme peut changer partiellement, mais il faut conserver inaltérés le contenu, l'identifiant, la structure et le contexte, parce qu'ils portent la cohérence du document. Nous traiterons dans la deuxième section du chapitre II les moyens pour remédier au changement constant des supports électroniques afin de garantir la conservation du contenu du document électronique.

907. Il convient de présenter un projet d'étude très ambitieux initié au Canada, qui porte le nom 'Projet InterPARES'[397] : il s'agit d'un projet de recherche sur la préservation à long terme de l'authenticité des documents d'archives numériques, crée par une équipe de recherches en sciences humaines au Canada. Ce projet a

---

[394] Charles KECSKEMETI et Lajos KORMENDY, *Op. cit.*.

[395] Lignes directrices à l'intention des créateurs, Projet InterPARES 2, p. 4. [En ligne : http://www.interpares.org/ip2/display_file.cfm?doc=ip2_creator_guidelines_booklet_french.pdf].

[396] Les documents dynamiques sont conçus pour optimiser l'affichage et la lisibilité. Au lieu d'avoir une disposition prédéfinie, ces documents ajustent et refluent dynamiquement leur contenu en fonction des variables d'exécution telles que la taille de la fenêtre, la résolution du périphérique et les préférences de l'utilisateur (en option). En outre, les documents dynamiques offrent des fonctionnalités de document avancées, telles que la pagination et les colonnes. Cette rubrique donne une vue d'ensemble des documents dynamiques et explique comment les créer. [En ligne : https://msdn.microsoft.com/fr-fr/library/aa970909(v=vs.110).aspx].

[397] Le projet InterPARES est principalement financé par le Conseil de recherches en sciences humaines du Canada ainsi que par la *National Historical Publications and Records Commission* et la *National Science Foundation* des États-Unis. Les fonds de contrepartie sont fournis par le *Hampton Fund Research Grant*, le Vice Président *Research Development Fund*, le doyen des Arts et la *School of Library, Archival and Information Studies* de l'Université de la Colombie-Britannique.
Pour obtenir de plus amples renseignements, visitez le site Web à l'adresse suivante : www.interpares.org.

élaboré des lignes directrices qui s'appliquent à divers types de publications, de documents et de données numériques ; ces lignes directrices sont particulièrement importantes pour les documents d'archives numériques.

908. Le projet InterPARES[398] a introduit des recommandations qui pourraient guider dans la création et la maintenance des documents numériques. Il a traité d'une manière particulièrement approfondie la question de l'intégrité, en lui attribuant une nouvelle définition: « *L'intégrité d'un document d'archives se réfère à sa complétude et à sa condition intacte : un document est intègre quand il est complet et inaltéré dans ses aspects essentiels.* »

909. De cette définition, nous trouverons une explication exhaustive de la notion de l''intégrité' et nous évoquons particulièrement l'expression « aspect essentiel » : *Ceci implique que son intégrité physique, tel que le nombre exact des chaines binaires, peut être modifiée, à condition que l'organisation du contenu, les annotations nécessaires, ainsi que les éléments de la forme documentaire restent les mêmes.*[399]

910. La littérature spécialisée s'intéresse surtout à l'intégrité des documents individuels, c'est-à-dire à la structure interne, et s'occupe peu de l'intégrité des agrégats de documents, c'est-à-dire de la structure externe. C'est peu judicieux parce qu'il y a des documents électroniques qui ne sont pas autonomes et leur présence ne suffit pas en soi; leur sens et leur valeur ne ressortent qu'en combinaison avec d'autres documents, tel que le cas en matière de documents négociables comme les connaissements maritimes électroniques dont l'opération de crédit par voie électronique exige l'examen de certains documents commerciaux pour vérifier la validité et la conformité du document électronique.

911. Il en résulte qu'il faut tenir compte de l'intégrité extérieure aussi bien que l'intégrité intérieure dans certains types de documents électroniques, tel est le cas de connaissement. Or, cette intégrité extérieure sera assurée lorsque nous

[398] *Ibid.*
[399] Conditions requises pour évaluer et maintenir l'authenticité des documents d'archives électroniques. InterPARES, p. 3. Il est à mentionner que les opinions données sur la forme documentaire divergent.

maintenons les liens entre les documents électroniques relevant d'une même opération ; et que le tri et l'élimination se font conformément au plan de classement et aux méthodes professionnelles, en coupant les liens qui n'ont plus intérêt d'exister lorsqu'ils ne sont plus valides et en donnant des précisions sur les critères de l'élimination.

912. **– Conclusion intermédiaire** – La preuve de l'intégrité d'un document électronique le rend ainsi singulier et unique. C'est ainsi que nous passons à la notion de l'unicité.

PARAGRAPHE 2 – L'UNICITÉ, NOTION GARANTISSANT LA CONFIANCE NUMÉRIQUE

913. La théorie classique des obligations nous dévoile une notion générale de l'unicité, chaque document transférable consigne les droits qu'il représente, et seul un document unique transférable peut représenter les droits qui y sont consignés ; ce qui implique nécessairement que tout transfert ou cession de ces droits par le porteur nécessite le transfert physique du document unique représentant physiquement ces droits[400].

914. De cette définition, un document juridique doit (quoique soit sa forme ou son type) avoir des caractéristiques que lui sont propres, lui permettant de se présenter comme unique dans le sens où la personne ne serait pas en mesure de le reproduire à sa seule discrétion, sans l'accord de l'autre partie avec qui elle a consenti l'acte.

915. Par souci de simplification, citons l'exemple d'une personne qui devrait recevoir le titre possessoire d'un instrument transférable ou d'un document titre par un message électronique ; dans cette hypothèse cette personne devra prendre toutes les mesures nécessaires pour s'assurer qu'aucun message identique n'a pu être envoyé à une tierce personne par une partie précédente faisant partie de la chaîne, ce qui donnerait à d'autres personnes la possibilité de revendiquer le titre.

---

[400] *Questions juridiques liées à l'utilisation des documents transférables électroniques*, '*A/CN.9/WG.IV/WP.115*', Commission des Nations Unies pour le droit commercial international, Groupe de travail IV (Commerce électronique), *Vienne*, 10-14 octobre 2011, p. 6.

916. Dans cet exemple, nous apercevons qu'une telle fuite incontrôlée d'information sur le système de sécurité et la reproduction non autorisée d'un 'document transférable électronique' pourraient donner à un porteur ou un bénéficiaire non autorisé le droit de demander la remise de marchandises ou le paiement d'une somme d'argent consignée dans le document.

917. Autre exemple, celui d'une lettre de change électronique confiée à un prestataire de services de confiance. Ce dernier veille à l'intégrité et l'unicité des documents électroniques et toutes données à caractère personnel à sa disposition. Il dispose de moyens techniques pour maintenir l'unicité des documents électronique de sorte que toute altération ou duplication du même document soit identifiée.

918. L'unicité est alors une exigence qui devrait être respectée indépendamment de la mise en circulation effective d'un 'document transférable électronique' afin d'empêcher la fraude et la mise en circulation de plusieurs documents concernant la même obligation. L'émission de plusieurs 'documents transférables électroniques' exposerait le débiteur à plusieurs demandes d'exécution et à la possibilité d'un paiement ou d'une livraison des biens à des personnes non habilitées à les recevoir. Ainsi pour éviter la survenance d'un tel événement regrettable, nous tenons à souligner l'importance de l'élaboration de mécanismes pour garantir l'unicité de ces instruments.

919. La garantie de l'unicité d'un document exige qu'il soit le seul qui existe ou bien, que toute copie soit clairement identifiable comme telle. Le caractère « identifiable » ne soulève pas de difficulté et signifie que le document est susceptible d'être identifié/ reconnu par l'usage de tel ou tel moyen, ce qui éviterait la possibilité de créer un double identique au premier et donc indifférenciable de celui-ci.

920. Le problème de la garantie de singularité est né en supposant que malgré les mesures adoptées pour sécuriser la transaction, un document électronique pourrait en général être copié d'une manière propre à créer un document identique au premier dont nous ne pourrons le différencier. En l'absence de

mesures particulières ou de l'application généralisée de technologies encore peu utilisées de nos jours, il n'y a guère de garantie ou certitude qu'un document électronique soit unique[401].

921. Il s'agit ainsi de s'interroger sur la nécessité de respecter l'"équivalence fonctionnelle" de la notion d'"unicité" (ou singularité) de la forme papier. Cette notion d'« équivalence fonctionnelle » est créée pour trouver les moyens alternatifs dans l'univers informatique que nous pourrons mettre en œuvre pour garantir l'unicité du document électronique.

922. Il convient de souligner que les documents papiers ne fournissent pas toujours une garantie absolue d'unicité. En fait, il peut ne pas être possible de trouver une définition législative unique de la notion d'unicité des documents papier. D'autre part, la fraude liée à la duplication illégale de ces documents est fréquente et d'autres problèmes peuvent être dus aux difficultés de rassembler l'ensemble des documents papier à présenter lorsque plusieurs originaux ont été émis.

923. Par conséquent, l'application d'une norme d'unicité plus stricte aux 'documents transférables électroniques' aux fins de répondre aux préoccupations susmentionnées et d'améliorer la sécurité pourrait être discriminatoire compte tenu du niveau de sécurité qu'offre leur équivalent papier, et risque en fin de compte de nuire à l'utilisation des 'documents transférables électroniques' dans la pratique commerciale.

924. Par ailleurs, il importe de reconnaître que l'exigence d'unicité d'un 'document papier transférable' (c'est-à-dire l'exigence de la garantie de singularité) est différente de celle qui prévoit qu'un tel document soit présenté ou conservé sous sa forme originale. La Loi type sur le commerce électronique[402] et la Convention sur les communications électroniques[403] conviennent de cette

[401] *Questions juridiques liées à l'utilisation des documents transférables électroniques*, *Op. cit.*, p. 6.
[402] Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation 1996, *Publication des Nations Unies, New York*, 1999.
[403] Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux, *Publication des Nations Unies, New York*, 2007.

distinction et, pour les transposer dans un environnement électronique, elles traitent de chacune de ces exigences séparément.

925. Les exigences juridiques qui prévoient que les documents soient présentés ou conservés sous leur forme originale sont traitées par la Loi type sur le commerce électronique (*art. 8)*[404] et la Convention sur les communications électroniques (*art. 9, par. 4)*[405] essentiellement comme des prescriptions en matière de preuve visant à garantir l'intégrité et la disponibilité des documents.

926. D'une part, selon la loi type sur le commerce électronique, il faut garder à l'esprit l'obligation de la communication de « l'original » de documents commerciaux tels que certificats de dépôt, certificats agricoles, certificats de quantité ou de qualité ou encore certificats d'assurance qui fait que la CNUDCI a adopté sa définition fonctionnelle de l'original[406].

927. La condition principale pour qu'il y ait original est qu'il existe une garantie fiable quant à l'intégrité de l'information (article 8, 1, a)[407]. CNUDCI précise que cette intégrité doit être appréciée en déterminant si l'information est restée

---

[404] Article 8 – Original de la Loi type de la CNUDCI sur le commerce électronique *1. Lorsque la loi exige qu'une information soit présentée ou conservée sous sa forme originale, un message de données satisfait à cette exigence : a) S'il existe une garantie fiable quant à l'intégrité de l'information à compter du moment où elle a été créée pour la première fois sous sa forme définitive en tant que message de données ou autre; et b) Si, lorsqu'il est exigé qu'une information soit présentée, cette information peut être montrée à la personne à laquelle elle doit être présentée.*
2. Le paragraphe 1 s'applique que l'exigence qui y est visée ait la forme d'une obligation ou que la loi prévoie simplement certaines conséquences si l'information n'est pas présentée ou conservée sous sa forme originale.
3. Aux fins de l'alinéa a du paragraphe 1 : a) L'intégrité de l'information s'apprécie en déterminant si celle-ci est restée complète et n'a pas été altérée, exception faite de l'ajout de tout endossement et de toute modification intervenant dans le cours normal de la communication, de la conservation et de l'exposition; et b) Le niveau de fiabilité requis s'apprécie au regard de l'objet pour lequel l'information a été créée et à la lumière de toutes les circonstances y relatives.
4. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes : [...].

[405] Article 9, par. 4 de la Convention des Nations Unies sur l'utilisation de communications prévoit que *« Lorsque la loi exige qu'une communication ou un contrat soit disponible ou conservé sous sa forme originale, ou prévoit des conséquences juridiques en l'absence d'un original, cette exigence est satisfaite dans le cas d'une communication électronique: a) S'il existe une garantie fiable quant à l'intégrité de l'information qu'elle contient à compter du moment où elle a été créée pour la première fois sous sa forme définitive, en tant que communication électronique ou autre; et b) Si, lorsqu'il est exigé que l'information qu'elle contient soit disponible, cette information peut être présentée à la personne à laquelle elle doit être rendue disponible ».*

[406] On remarquera que la notion semble différer de ce que le droit belge appelle « original ». En effet, la condition pour qu'un document soit original dans le droit français est qu'il soit signé, ce qui n'est pas nécessairement le cas dans le système de la loi type.

[407] *Ibid.*

complète et n'a pas été altérée (art. 8.,3., a)[408], mais que le niveau de fiabilité requis dépend des circonstances (art. 8., 3., b)[409].

928. D'autre part, d'après l'article 9, par. 4 de la Convention sur les communications électroniques[410], l'exigence de conserver une communication ou un contrat sous sa forme originale doit répondre à un double critère:

a) une garantie fiable de l'intégrité de l'information et du contenu du document en question ;
b) l'information exigée est disponible, et peut être présentée à la personne à laquelle elle doit être rendue disponible.

929. Là encore, dans les deux cas nous nous servons de l'équivalence fonctionnelle pour déterminer les critères de l'original. Nous retenons ainsi une double exigence qui est d'un côté la nécessaire intégrité durant tout le cycle de vie du document, et que l'original soit accessible et disponible pour la personne ayant droit à réclamer ses droit en détenant ce document.

930. Dans ce sens, lorsque nous envisageons le cas de figure d'un document électronique, ces exigences précitées sont satisfaites: 1) s'il existe une garantie fiable quant à l'intégrité de l'information, et 2) si l'information peut être présentée aux personnes appropriées. Selon cette approche, nous pouvons admettre que plusieurs copies de la même communication électronique peuvent être considérées comme étant sous leur forme originale, dans la mesure où nous respectons la double exigence susmentionnée de validité.

931. En matière de la lettre de change électronique, nous répondons aux deux exigences précitées de la manière suivante : d'une part, le bénéficiaire du titre doit être en mesure de disposer du document pour réclamer ses droits ; et d'autre part le prestataire du service de confiance doit garantir l'intégrité et l'unicité de la lettre de change qui lui a été confiée.

[408] *Supra.*
[409] *Supra.*
[410] *Supra.*

932. L'emploi d'une méthode fiable de transfert de données devient un pré-requis ; la garantie de l'unicité d'un document exige qu'il soit le seul qui existe (ou bien, que toute copie soit clairement identifiable comme telle). Dans ce sens, l'*article 17* de la Loi type sur le commerce électronique[411] reconnaît la nécessité de régler la question de l'unicité dans le contexte des documents de transport électroniques ; pourtant elle n'a pas précisé comment y parvenir, elle exige uniquement qu'"*une méthode fiable soit utilisée pour rendre unique le message ou les messages en question*".

933. Cette dernière expression doit être comprise comme faisant référence à « *l'emploi d'une méthode fiable pour veiller à ce que les messages de données devant transmettre tout droit ou obligation d'une personne ne puissent pas être utilisés par cette personne d'une manière contraire à tout autre message de données par lequel cette personne a transmis le droit ou l'obligation* »[412].

934. Par exemple, une lettre de change ou un chèque, aussi en papier qu'en version électronique, peut changer de bénéficiaire à plusieurs reprises au cours de sa vie ; ceci grâce au mécanisme de l'endossement qui permet de transmettre le titre ainsi que les droits dont il dispose d'une personne à une autre. Dans cette hypothèse de transmission de titre électronique par endossement, l'emploi d'une

---

[411] Article 17 de la Loi type de la CNUDCI sur le commerce électronique. « ***1.*** *Sous réserve des dispositions du paragraphe 3, lorsque la loi exige qu'un acte visé à l'article 16 soit exécuté par écrit ou au moyen d'un document papier, cette exigence est satisfaite si l'acte est exécuté au moyen d'un ou de plusieurs messages de données.* ***2.*** *Le paragraphe 1 s'applique que l'exigence qui y est visée ait la forme d'une obligation ou que la loi prévoie simplement certaines conséquences si l'acte n'est pas exécuté par écrit ou au moyen d'un document papier.* ***3.*** *Quand un droit doit être dévolu à une personne et à aucune autre, ou quand une obligation doit être acquise par une personne et aucune autre, et si la loi exige à cette fin que le droit ou l'obligation soient transmis à l'intéressé par le transfert ou l'utilisation d'un document papier, cette exigence est satisfaite si le droit ou l'obligation en question sont transmis par un ou plusieurs messages de données, à condition qu'une méthode fiable soit utilisée pour rendre uniques le message ou les messages en question.* ***4.*** *Le niveau de fiabilité requis aux fins du paragraphe 3 s'apprécie au regard de l'objet pour lequel le droit ou l'obligation ont été transmis et à la lumière de toutes les circonstances, notamment de toute convention en la matière.* ***5.*** *Lorsqu'un ou plusieurs messages de données sont utilisés pour exécuter l'un des actes mentionnés aux alinéas f et g de l'article 16, aucun document papier utilisé pour exécuter cet acte n'est valide à moins que l'utilisation de messages de données n'ait été abandonnée et remplacée par l'utilisation de documents papier. Tout document papier émis dans ces conditions doit contenir la notification de ce remplacement. Celui-ci est sans effet sur les droits ou les obligations des parties.* ***6.*** *Si une règle de droit est impérativement applicable à un contrat de transport de marchandises qui figure dans un document papier ou est constaté par un document papier, cette règle n'est pas rendue inapplicable à un tel contrat de transport de marchandises qui est constaté par un ou plusieurs messages de données par le seul fait que le contrat est constaté par de tels messages et non par un document papier.* ***7.*** *Les dispositions du présent article ne s'appliquent pas dans les situations suivantes : [...].* »

[412] Guide pour l'incorporation dans le droit interne de la loi type de la CNUDCI sur le commerce électronique, *op. cit.*, n° 117.

méthode fiable est primordial pour veiller à ce que le titre électronique soit transmis au nouveau bénéficiaire, et que seulement ce dernier qui pourra réclamer les droits qui lui a été transmis en détendant le titre.

935. Afin de garantir d'avantage l'unicité de documents de transport, article 17 (5)[413] a mis en place un système pour éviter le double emploi ou la contradiction entre actes papier et messages de données pour certains documents de transport. Le système consiste à interdire d'utiliser des documents papier une fois que des messages de données ont été utilisés, sauf à notifier expressément le changement de support.

936. Par ailleurs, l'*article 9* des Règles de Rotterdam[414] traite aussi indirectement la même question en exigeant que "*l'utilisation d'un document électronique de transport négociable soit soumise à des procédures*" définies par les parties et en identifiant quatre catégories de questions devant en partie régler les problèmes d'unicité :

- Une méthode précise pour émettre le document en faveur du porteur envisagé et le lui transférer;
- Des moyens opportuns pour assurer que le document conservera son intégrité;
- La façon dont le porteur peut démontrer qu'il a la qualité de porteur;
- La façon de confirmer que la livraison au porteur a eu lieu.

937. Pourtant, à l'instar de la Loi type sur le commerce électronique, les Règles de Rotterdam ne précisent pas comment ces procédures doivent être appliquées. En revanche, bien que les auteurs de la Convention sur les communications électroniques sont également convenus que l'unicité est indispensable pour les 'documents transférables électroniques', ils ont reconnu que, pour trouver une solution, il fallait recourir à une combinaison de solutions juridiques, techniques et commerciales qui n'étaient pas encore entièrement au point ni éprouvées. Ainsi la Convention sur les communications électroniques a exclu de son champ

[413] ***Supra**, voir paragraphe n°932.*

[414] Convention des Nations Unies sur le contrat de transport international de marchandises effectué entièrement ou partiellement par mer (les "Règles de Rotterdam"), adoptée par l'Assemblée générale le 11 décembre 2008, *Publication des Nations Unies, Vienne*, 2009.

d'application la question relevant de la validité des 'documents transférables électroniques'[415].

938. Par conséquent, il fallait chercher en dehors de la Convention sur les communications électroniques pour trouver un mécanisme de gestion de documents fonctionnellement équivalent afin de satisfaire à l'exigence d'unicité ou de singularité des 'documents transférables électroniques'.

939. À cet égard, il importe de noter que la fonction d'unicité ou de singularité doit donner des assurances suffisantes qu'un seul créancier puisse revendiquer le droit à l'exécution de l'obligation consignée dans le document. Nous pourrons y parvenir en éliminant la possibilité que circulent plusieurs documents applicables consignant le même droit.

940. **Conclusion intermédiaire –** lorsqu'on a envisagé la théorie de l'unicité d'un document électronique, nous retenons que pour obtenir l'unicité technique, il faut satisfaire au double critère : de la fiabilité du document, et son originalité dans le sens où seulement la personne ayant droit pourra l'utiliser. Il est d'ailleurs nécessaire de trouver l'outil pour permettre à ce document électronique qu'il soit l'exemplaire faisant foi.

[415] Voir Convention sur les communications électroniques, article 2, paragraphe 2; voir également *A/CN.9/571*, par. 136.

SECTION 2 – LA SÉCURISATION DE L'USAGE PAR LA DÉSIGNATION D'UN EXEMPLAIRE FAISANT FOI.

941. La désignation d'un exemplaire qui fait foi du document transférable électronique, indépendamment du nombre d'autres exemplaires existants, peut répondre aux préoccupations concernant l'intégrité du document.

942. En théorie et vu l'avancement rapide des moyens technologiques de la protection des données, il est devenu techniquement possible aujourd'hui de suivre la technologie en cours et créer un document électronique réellement unique qui ne peut pas être copié (du moins sans que nous ne puissions distinguer la copie de l'original) et qui peut être transféré en toute sécurité.

943. Si nous supposons que la technologie actuelle soit capable d'assurer l'unicité d'un document électronique et de permettre son transfert, elle fournirait ainsi une base pour rendre un document électronique unique, c'est-à-dire capable de reproduire un document papier unique tout en gardant son caractère original.

944. Parmi les technologies, qui permettraient d'assurer cette unicité technique, figurent en premier lieu le mécanisme de la conservation des documents électroniques dans un système sécurisé spécifique (***Paragraphe I)***. Puis il y a les systèmes de gestion des documents électroniques qui peuvent être utilisés pour la désignation d'un exemplaire faisant foi ; de ces systèmes de gestion figure l'identifiant d'objet numérique (DOI) et la gestion des droits numériques (DRM). (***Paragraphe II)***.

PARAGRAPHE I : DÉSIGNATION D'UN EXEMPLAIRE REPOSANT SUR LA CONSÉRVATION DANS UN SYSTÈME SECRURISÉ SPÉCIFIQUE.

945. Cette première approche consiste à conserver une copie du 'document transférable électronique' désignée comme exemplaire faisant foi dans un système informatique sécurisé conçu à cet effet et protégé par des contrôles de sécurité et d'accès appropriés[416].

946. Dans ce cas de figure, nous mettons en œuvre un système d'information spécialement conçu pour stocker un type particulier de 'documents transférables électroniques', et en conserver la trace pour un secteur d'activité donné. En suivant cette hypothèse, l'exemplaire faisant foi du 'document transférable électronique' reste conservé dans le système désigné pendant toute sa durée de vie. De cette approche, l'unicité d'un document électronique est assurée par l'instauration d'un environnement sécurisé dans lequel un exemplaire du document électronique peut être conservé.

947. Les mesures de contrôle du système assurent que l'intégrité du document reste préservée, indépendamment de l'endroit ou de la manière dont il est stocké dans le système, ou même du nombre d'exemplaires qui y figurent.

948. Citons l'exemple d'une lettre de change électronique dont nous avons conservé une copie pour être un exemplaire faisant foi dans un système informatique sécurisé. Grâce à cette méthode, nous disposons d'une pièce de référence dont nous aurons recours en cas de violation or falsification du titre, et nous serons capables de conserver la trace de la lettre de change électronique pendant toute la durée de sa vie.

[416] *Questions juridiques liées à l'utilisation des documents transférables électroniques*, *Op. cit.*, p. 12.

PARAGRAPHE II : DÉSIGNATION D'UN EXEMPLAIRE REPOSANT SUR UN CONTENU VÉRIFIABLE ET TRACABLE

949. Nous traitons ici les systèmes qui pouvaient être mis en œuvre dans la pratique pour l'émission et le transfert de documents électroniques : il s'agit de créer des systèmes de gestion de l'information qui permettent aux utilisateurs de localiser, grâce à la technologie et aux communications, l'endroit où l'exemplaire faisant foi est stocké.

950. Pour ce qui est des solutions techniques, nous classerons ainsi les systèmes de gestion des documents numériques en deux catégories, celle des registres et celle des plates-formes de transaction. Nous envisagerons en détail la méthode du Registre dans un deuxième chapitre, et nous nous contentons plutôt ici à traiter la méthode des plates-formes de transaction.

951. La méthode de la plate-forme de transaction est une méthode de gestion des documents électroniques qui repose essentiellement sur une technologie permettant de garantir l'unicité du document électronique et d'en autoriser le transfert. Dans ce cas de figure, l'entité qui contrôle l'objet pouvait être identifiée comme détentrice du document électronique, avec tous les droits qui en découlent. Dans ce cadre, nous visons 2 dispositifs techniques de protection des documents électroniques, l'un est l'identifiant d'objet numérique (DOI) (I) et l'autre est la gestion des droits numériques (DRM) (II).

I. L'identifiant d'objet numérique (*DOI – « Digital Object Identifier*»)[417]

952. Il s'agit d'une nouvelle norme internationale qui fournit un système pour attribuer un identifiant international unique attribué aux objets voués à une utilisation sur les réseaux numériques. Le système d'identificateur d'objet numérique [DOI®] fournit une infrastructure pour l'identification unique persistante d'objets de tout type.

[417] En ligne : http://www.doi.org/.

953. Cette nouvelle technique devrait bénéficier aux éditeurs, gestionnaires de contenus, distributeurs multimédias, archivistes, associations œuvrant pour le patrimoine culturel, ainsi qu'au secteur de la technologie d'internet et les 'documents transférables électroniques'.

954. Ces identifiants uniques DOI jouent un rôle indispensable dans la gestion de l'information, et ce dans tout environnement numérique. En effet, le système DOI est conçu comme un cadre général applicable au moindre objet numérique, auquel il donne un moyen d'identification, de description et de résolution structuré et extensible.

955. Le système DOI a été lancé en 1998 par l'*International DOI Foundation* (IDF) – une organisation à but non lucratif, et l'Autorité qui détient l'enregistrement pour la norme ISO 26324[418]. ISO 26324 est l'instrument par lequel le système DOI a été adopté comme norme internationale et IDF nommé l'Autorité d'enregistrement 26324 ISO.

956. Cette norme internationale *ISO26324:2012, Information et documentation – Système d'identifiant numérique d'objet*[419] fut publiée par l'ISO (Organisation internationale de normalisation), offre un moyen efficace d'identifier une entité sur Internet et est utilisée principalement pour l'échange au sein d'une communauté d'utilisateurs intéressés et la gestion de la propriété intellectuelle[420].

957. Ainsi le DOI est le cœur d'un mécanisme d'identification de ressources numériques, comme les revues, articles scientifiques, rapports, vidéos, etc. Il est parfois comparé aux ISSN[421] ou ISBN[422] pour le web, mais c'est aussi une

---

[418] Elizabeth Gasiorowski-Denis, *l'identifiant numérique d'objet (DOI) devient une norme ISO*, le 10 mai 2012, [En ligne : http://www.iso.org/iso/fr/home/news_index/news_archive/news.htm?refid=Ref1561].

[419] ISO 26324:2012, *Information et documentation – Système d'identifiant numérique d'objet*, a été élaborée par le comité technique ISO ISO/TC 46, *Information et documentation*, sous-comité SC 9, *Identification et description*. Elle est disponible auprès des instituts nationaux membres de l'ISO. Il est aussi possible de l'obtenir directement au Secrétariat central de l'ISO, au prix de 92 francs suisses, par l'intermédiaire de l'ISO Store ou en contactant le Département Marketing, Communication & Information.

[420] Elizabeth Gasiorowski-Denis, *Ibid.*

[421] L'*International Standard Serial Number* (ISSN) ou numéro international normalisé des publications en série est le numéro international qui permet d'identifier de manière unique une publication en série. Il concerne donc les journaux, les revues et les collections de monographies, quel que soit le support. Au-delà de son rôle d'identification des titres, l'ISSN est un outil essentiel pour la gestion des périodiques pour

alternative à l'instabilité des URL par l'association de la localisation du document et des métadonnées qui lui sont liées.

958. Un nom DOI est l'identifiant d'une entité donnée – physique, numérique ou abstraite – sur des réseaux numériques. Il rassemble des informations sur un objet, notamment l'emplacement de cet objet ou les informations s'y rapportant, qui peuvent se trouver sur l'Internet[423].

959. Le système DOI est conçu pour fonctionner sur Internet. Un nom DOI est affecté en permanence à un objet pour fournir une liaison réseau persistante à l'information actuelle sur cet objet, y compris lorsque l'objet ou de l'information à ce sujet, peut être trouvé sur Internet. Bien que des informations sur un objet puissent changer au fil du temps, son nom de DOI ne changera pas.

960. Les applications du système DOI comprennent la gestion de la localisation de l'information et de la documentation ainsi que de son accès, la gestion des métadonnées, la facilitation des transactions électroniques, l'identification unique persistante de toute donnée sous toute forme, et les transactions commerciales et non commerciales. Ainsi le système DOI a été conçu dans un souci d'interopérabilité, au sens où il peut être utilisé ou fonctionner avec des identifiants et des schémas de métadonnées existants.

961. Théoriquement, il est possible d'affecter un nom DOI à un 'document transférable électronique' qui existe sur Internet, tels que le chèque ou un billet à ordre, pour établir l'identification unique du titre. Ceci pourra garantir l'intégrité et l'unicité du document électronique.

---

l'archivage électronique, le catalogage, la distribution, la gestion des abonnements et la numérisation. Les monographies emploient quant à elles la numérotation ISBN. L'ISSN est normalisé par le texte ISO 3297:2007 (ICS n° 01.140.20) et dépend du comité technique ISO/TC46 (Information et documentation). Initialement publié en 1975, le texte officiel a été révisé en 1986, 1998 et 2007. Cette norme peut être commandée sur le site de l'ISO.

[422] L'*International Standard Book Number* (ISBN) ou Numéro international normalisé du livre (NINL) est un numéro international qui permet d'identifier, de manière unique, chaque édition de chaque livre publié, que son support soit numérique ou sur papier. Il est destiné à simplifier la gestion informatique pour tous les intervenants de la chaîne du livre (imprimeur, éditeur, libraire, bibliothèque, etc.).

[423] En ligne : http://www.doi.org/doi_handbook/1_Introduction.html.

II. La gestion numériques des droits (GND), (traduit de l'anglais : *DRM « Digital Rights Management »*).

962. Pour un 'document transférable électronique', ce système de gestion des droits donne un accès limité aux documents. Il permet la vérification de l'identité de la personne ayant les droits consignés sur le document, tout en ne permettant pas à quiconque de changer le contenu du document électronique.

963. DRM est l'abréviation anglaise de *Digital Rights Management* ; en français, la gestion numérique des droits ou gestion des droits numériques (GND). Il s'agit d'un dispositif technique de protection ayant pour objectif de contrôler l'utilisation qui est faite des œuvres numériques ainsi que de protéger ces derniers contre un usage non autorisé[424]. Ce dispositif peut s'appliquer à tous types de supports numériques physiques (disques, DVD, Blu-ray, logiciels, etc.) ou de transmission (télédiffusion, services Internet, etc.) grâce à un système d'accès conditionnel[425].

964. La technologie DRM est utilisée généralement par les fournisseurs de contenu tels que les magasins en ligne pour contrôler la façon dont les fichiers numériques audio ou vidéo qu'ils procurent sont utilisés et distribués.

965. Dans ce sens, les droits d'utilisation du média sont des autorisations accordées qui permettent d'utiliser un fichier protégé d'une certaine manière. Les fournisseurs de contenu ont la possibilité de spécifier la façon dont le client pourrait utiliser les fichiers protégés qu'ils leur procurent.

966. Un fournisseur de contenu peut ainsi par exemple octroyer à l'utilisateur l'autorisation d'écouter le fichier sur son ordinateur (droit de lecture), de le graver sur un CD audio (droit de gravure) ou de le synchroniser sur un périphérique mobile (droit de synchronisation)[426].

---

[424] Guide de la gestion des droits numériques à l'usage des consommateurs, Digital Management. Etes-vous vraiment informé?, une publication du projet INDICARE, [En ligne : http://www.indicare.org/tiki-download_file.php?fileId=196].

[425] L'identifiant numérique d'objet (DOI) devient une norme ISO, Elizabeth Gasiorowski-Denis, le 10 mai 2012, En ligne : http://www.iso.org/iso/fr/home/news_index/news_archive/news.htm?refid=Ref1561.

[426] Gestion des droits numériques (DRM) du Lecteur Windows Media : Forum Aux Questions, [En ligne :

967. Citons par exemple que dans le système d'exploitation *Windows*, le Lecteur *Windows Media* ainsi que certains magasins en ligne et les périphériques prennent en charge ou utilisent une sorte de DRM appelée *Windows Media Digital Rights Management*[427].

968. Ainsi un fichier auquel la gestion des droits numériques a été appliquée est un fichier protégé et que le client ne pourrait pas l'utiliser en dehors du cadre du droit ou privilège que lui était accordé par le fournisseur de contenu.

969. En suivant cet exemple, chaque droit a certaines caractéristiques. Ainsi, le fournisseur de contenu peut accorder à l'utilisateur les droits d'utilisation suivants :

- le droit d'écouter (droit d'utilisation) une chanson précise sur votre ordinateur un nombre illimité de fois ;
- le droit de synchroniser cette chanson avec deux appareils mobiles cinq fois par mois ;
- le droit de graver deux fois la chanson sur un CD audio.

970. Au vu de ce qui précède, le dispositif technique DRM peut viser en général les options suivantes :

- restreindre la lecture du support à une zone géographique prévue (par exemple les zones des DVD) ;
- restreindre la lecture du support à du matériel spécifique (par exemple les versions smartphone ou tablette) ;
- restreindre la lecture du support à un constructeur ou vendeur (afin de bloquer la concurrence) ;
- restreindre ou empêcher la copie privée du support (transfert vers un appareil externe) ;
- restreindre ou verrouiller certaines fonctions de lecture du support (désactivation de l'avance rapide sur certains passages d'un DVD). Très utile pour obliger l'exposition aux annonces publicitaires ;

---

http://windows.microsoft.com/fr-fr/windows/media-player-drm-faq#1TC=windows-7].

[427] *Ibid.*

- identifier et tatouer numériquement toute œuvre et tout équipement de lecture ou enregistrement (pour faciliter le pistage des copies non autorisées, mais surtout empêcher la personnalisation et donc le contrôle d'une technologie, par exemple empêcher l'installation d'un autre système d'exploitation sur un ordinateur).

971. Techniquement, le dispositif *DRM* exploite un chiffrement de l'œuvre, combiné à un accès conditionnel. L'éditeur ou le distributeur qui exploite ce contrôle d'accès ne confie la clé de contrôle d'accès du produit, qu'en échange d'une preuve d'achat ou de souscription pour y accéder (par exemple pour l'abonnement à une chaîne payante, vidéo à la demande (VOD), téléchargement, etc.). L'accès à la lecture (et/ou sa copie) du document ainsi protégé n'est alors autorisée que pour l'équipement ou l'identification logicielle certifiée par le fournisseur.

972. Pour conclure, le dispositif *DRM* est une technique qui dispose d'un chiffrement qui limitera l'accès des données aux personnes autorisées, en accordant à chaque personne le niveau d'accès dont il a le droit. Bien que dispositif de protection n'ait pas encore utilisé pour la gestion du 'document transférable électronique', ce dernier pourra bénéficier de *DRM* pour contrôler leur accès.

973. La notion de "mesures techniques de protection" a été introduite en France par la *Loi du 1er août 2006* relative au droit et aux droits voisins dans la société de l'information. D'après l'article *L. 331-5 de la Loi du 1er aout 2006,* nous entendons par mesure technique *toute technologie, dispositif, composant qui, dans le cadre normal de son fonctionnement, accomplit la fonction prévue par cet alinéa*. Le législateur français a précisé d'avantage que « *ces mesures techniques sont réputées efficaces lorsqu'une utilisation (...) est contrôlée par les titulaires de droits grâce à l'application d'un code d'accès, d'un procédé de protection tel que le cryptage, le brouillage ou toute autre transformation de l'objet de la protection ou d'un mécanisme de contrôle de la copie qui atteint cet objectif de protection* ».

974. Par cette définition, la loi reconnait le terme « mesures techniques de protection » que nous pouvons désormais mettre en œuvre pour les '*documents transférables électroniques*' en leur donnant un moyen d'identification techniquement et juridiquement efficace grâce à ces mesures techniques de protection (*DOI* ou *DRM*).

975. Du point de vue juridique, les notions qui consacrent les mesures techniques de protection existent dans le droit ; que ces mesures bénéficient d'une protection légale, aussi bien au niveau local qu'international.

976. La notion de « mesures techniques de protection » est traitée aux Etats-Unis dans Le *Digital Millennium Copyright Act (DMCA)*[428]. Il s'agit d'une loi américaine adoptée en 1998 ayant pour objectif de fournir un moyen de lutte contre les violations du droit d'auteur ; qu'elle vise à établir une législation de la propriété intellectuelle adaptée à l'ère numérique.

977. Parmi les dispositions contenues dans la *DMCA*, il y a la possibilité d'interdire explicitement le contournement des technologies utilisées pour protéger les documents assujettis au droit d'auteur. Cette législation américaine interdit aussi le détournement d'une protection contre la copie en empêchant l'ingénierie à rebours des mesures techniques de protection et ainsi la lecture par tout matériel d'œuvres ainsi protégées, acquises de manière régulière[429]. L'équivalence européenne de *DMCA* est *l'EUCD*[430] et la transcription en France est la loi *DADVSI*, qui a été adoptée le 1er août 2006.

978. Il importe aussi d'évoquer le fait que ces mesures technologiques ont provoqué la polémique sur leur efficacité pratique, car elles peuvent restreindre la lecture des œuvres, au seul équipement certifié par le diffuseur et que des dispositifs concurrents pouvant être incompatibles entre eux. Elles sont accusées ainsi d'engendrer des situations de monopole et de non concurrence. Que malgré

[428] *The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary*, December 1998. [En ligne : http://copyright.gov/legislation/dmca.pdf].
[429] The Digital Millennium Copyright Act of 1998, *Ibid.*
[430] La Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, *Journal officiel* n° L 167 du 22/06/2001 p. 0010 - 0019.

ce que leur nom pourrait laisser entendre, les DRM sont une contrainte technique et non légale[431].

979. – Conclusion intermédiaire – Nous avons traité le critère de contrôle, et la désignation d'un exemplaire faisant foi, afin de reconnaitre une équivalence fonctionnelle de l'unicité matérielle attachée aux documents papiers ; cette exigence d'unicité n'est pas la seule en droit des biens ; il existe aussi l'exigence de la possession caractérisée par la détention matérielle du document par la personne ayant droit.

[431] Pour plus d'informations, consulter le guide de la Gestion des Droits Numériques à l'Usage des Consommateurs, publié en avril 2006 sur le site http://www.indicare.org/consumer-guide/

CONCLUSION DU CHAPITRE I

980. L'objectif de l'unicité technique du 'document transférable électronique' est d'adopter une méthode fiable pour garantir que seul un document unique transférable existe pour représenter les droits qui y sont consignés, et que personne ne pourra reproduire le document électronique à l'insu des parties contractantes. Le respect de l'unicité technique suppose que le contenu du document électronique reste intact, complet, et sans altération, que le document soit mis à la disposition des personnes qui y ont droit.

981. Nous constatons qu'il est possible d'établir la sécurisation de l'usage du document électronique par le biais de la désignation d'un exemplaire faisant foi. D'une part la conservation du document électronique peut être le fait d'un système spécifique sécurisé (application logicielle interne à l'entreprise). Dans ce cas, nous disposons d'un document électronique enregistré sur le système, pour servir de référence afin de distinguer la copie de l'original.

982. D'autre part, le recours à un système de gestion externe à l'entreprise est possible sur une plateforme permettant l'identification de ce document.

Dans cette approche, nous disposons de deux systèmes :

- Le recours à l'identifiant d'objet numérique (DOI) : Le mot « DOI » est intégré techniquement dans le document à l'aide d'un lien hypertexte et garantit la disponibilité du document sans la moindre altération de contenu.
- Le recours à un système de gestion des droits numériques (DRM) : c'est une plateforme qui peut fournir un accès limité pour le besoin de la vérification de l'identité de la personne qui utilise le document électronique. Ce dernier système est plus adapté aux œuvres multimédias, les magasins en ligne, ou encore le service de la vidéo sur demande.

En conclusion les entreprises ont plus facilement recours à une plateforme externe, et c'est celle du DOI qui est généralement choisie car plus adaptée.

CHAPITRE 2

L'ÉQUIVALENCE FONCTIONNELLE DE LA POSSESSION MATERIELLE

983. Outre le traitement de la question de la singularité et l'unicité, la définition d'un mécanisme fonctionnellement équivalent nécessaire pour satisfaire à l'exigence de la possession d'un 'document transférable électronique' constitue un autre défi majeur pour l'opérabilité et l'exécution de ces derniers.

984. Pour ce faire il faut concevoir un processus dans lequel le porteur qui invoque un transfert régulier d'un 'document transférable électronique' ait l'assurance qu'il existe bien un 'document transférable électronique' unique et qu'il est techniquement possible de mettre en œuvre un mécanisme de contrôle de ce document équivalent en droit à sa possession matérielle.

985. Etant une preuve efficace de singularité, cette exigence relative à la possession du document manuscrit protège l'émetteur aide à assurer le bénéficiaire du transfert (le porteur) qu'il a acquis un titre valable et protège ce dernier contre le transfert frauduleux d'un duplicata.

986. Ici nous nous posons la question de savoir comment nous allons établir de nouveaux critères d'équivalence pour les fonctions remplies par les documents papier. Nous pouvons choisir entre deux moyens pour satisfaire à cette nécessité, soit adopter une norme unique générale et souple susceptible de remplir l'ensemble des fonctions du document papier dans un environnement électronique, soit émettre des normes distinctes visant à remplir chacune de ces fonctions.

987. Dans un premier temps, nous traiterons le critère de la possession sur les documents transférables électroniques, et nous trouverons un équivalent fonctionnel susceptible d'application à ces derniers ; ceci pourra être établi au moyen de la notion de contrôle qui est utilisé comme équivalent fonctionnel de la possession. (*section 1 : Le critère du contrôle comme substitut de la possession matérielle*). Dans un second temps, nous envisageons l'identification de la personne qui pourra se prévaloir de la valeur/de l'obligation qu'il représente (*section 2 : L'identification du porteur du 'document transférable électronique'*).

SECTION 1 – LE CRITÈRE DU CONTROLE COMME SUBSTITUT DE LA POSSESSION MATERIELLE

PARAGRAPHE I – L'APPLICATION DE LA "POSSESSION" NOTION DE DROIT PRIVÉ

988. En droit civil, et plus précisément en droit des biens, l'aspect matériel de la possession est essentiel pour caractériser le bien. La possession n'est pas un nouveau concept en droit privé, ayant des origines lointaines qui relèvent du droit romain[432], ses racines l'ont plongé dans une matérialité dont nous avons du mal à sortir. Cet aspect matériel inhérent à la possession l'a longtemps rendu inapte à suivre l'évolution du droit des biens vers l'immatériel.

I. L'inadéquation de la notion classique de "possession" de droit des biens aux biens immatériels

A. Notion de la possession

989. En droit des biens, la possession est considérée comme un état de fait exclusif de toute situation de droit. Elle est définie comme l'*exercice d'un droit, indépendamment de sa titularité*. De cette définition nous saisissons deux aspects dominants de la possession :

990. D'une part, la possession est présentée comme l'exercice d'un droit. Cet exercice reflète un élément factuel car la possession est ici un fait et non un droit ; que cet exercice de droit est envisagé indépendamment de la question de sa légitimité.

991. Quoi que soit la nature juridique de la possession, peu importe qu'elle soit obtenue de façon légitime ou non, est indiffèrent tant que la possession factuelle

[432] KARL VON SAVIGNY (F.), *Traité de la Possession en Droit romain*, traduit de l'allemand par CH. Faivre D'Audelange, *Imprimerie De Cosse et Gaultier-Laguionie*. 6e Édition 1841.

de la chose est exercée par une personne physique. Il ne s'agit pas là d'une prérogative juridique, mais simplement un pouvoir de fait sur un bien. Cela signifie que la possession n'est pas nécessairement l'exercice d'un droit par son titulaire, et que cela pourrait être l'exercice ou le recours à la force d'un usurpateur pour s'approprier du bien[433].

992. Ainsi, dès l'instant que la possession est indifférente à la titularité du droit exercé et qu'elle contente uniquement à son exercice concret, elle est plongée dans la factualité et la matérialité. Cette interprétation est confortée par la quasi-unanimité des auteurs qui perçoivent la possession comme un fait, pas une prérogative de droit[434].

993. En admettant qu'il s'agit d'un exercice factuel, cela ne met pas en cause la nature juridique de la possession ; étant un fait juridique dans la mesure où la loi en fait découler un certain nombre de conséquences juridiques, dont la principale est l'acquisition du droit possédé par l'écoulement du temps, voire de manière immédiate dans le cadre de l'article 2276 du Code civil[435].

994. Ce texte de l'article 2276 C.civ prévoit une période de prescription de 3 ans pour revendiquer un meuble volé ou perdu ; qu'au delà de cette période, l'ancien titulaire ne sera plus en mesure de réclamer la propriété du bien qu'il détenait. C'est ce qui s'appelle la prescription acquisitive (« Usucapion »)[436] qui permet au possesseur d'invoquer le bénéfice de l'usucapion[437].

---

[433] Comp. F. Terré et Ph. Simler, *op. cit., n° 152* : la possession "est le fait par une personne d'accomplir des actes qui, dans leur manifestation extérieure, correspondent à l'exercice volontaire d'un droit, qu'elle soit ou non titulaire de ce droit".

[434] William Dross, *Fasc. unique : Prescription Acquisitive - Possession, JurisClasseur Civil Code*, 20 Février 2013, n° 9.

[435] Article 2276 du Code Civil prévoit que : « *En fait de meubles, la possession vaut titre. Néanmoins, celui qui a perdu ou auquel il a été volé une chose peut la revendiquer pendant trois ans à compter du jour de la perte ou du vol, contre celui dans les mains duquel il la trouve ; sauf à celui-ci son recours contre celui duquel il la tient* ».

[436] Les critères de l'usucapion sont les suivants :

Existence d'une possession véritable : cela s'explique par le fait qu'un simple détenteur précaire ne peut invoquer le bénéfice de l'usucapion. C'est essentiel pour une prescription acquisitive de porter sur une possession, non une détention précaire. Une possession utile : Pour permettre la prescription, la possession doit revêtir les caractères énoncés par l'article 2261 du Code civil436 qui stipule quatre (4) conditions contre les vices : discontinuité, violence, clandestinité et équivoque.

B. Éléments constitutifs de la possession en droit des biens

995. La possession est la réunion de deux éléments de nature différente, l'un matériel ou objectif (le *corpus)* et l'autre est intellectuel ou subjectif (l'*animus).* Cette distinction, d'origine romaine demeure pertinente et applicable de nos jours[438]. Etant l'aspect objectif et matériel de la possession, le *corpus* est l'élément constitutif le plus débattu ; que les débats judiciaires portent souvent sur sa seule caractérisation.

996. Lorsque la possession est désignée par l'exercice d'un droit, elle suppose forcément l'accomplissement d'actes concrets pour traduire cet exercice. Ce sont ces actes d'exercice qui sont désignés sous le terme de *corpus*, sans lesquels il ne saurait y avoir de possession.

997. Dans ce sens, les professeurs Aubry et Rau donnent plus de précision à l'aspect matériel de la possession, en précisant que " *nous appelons possession dans le sens le plus large de cette expression, l'état ou la relation de fait qui donne à une personne la possibilité physique, actuelle et exclusive, d'exercer sur une chose des actes matériels d'usage, de jouissance et de transformation*"[439].

998. Nous retenons de cette définition que le *corpus* se caractérise par des actes d'exercice du droit, lesquels sont conditionnés par la nature de la chose objet du

---

- Une possession continue et non interrompue : Le possesseur doit accomplir périodiquement des actes que tout propriétaire normalement diligent accomplirait. Que la discontinuité de la possession fait défaut de possession.
- Une possession paisible : la possession doit être sereine et purgée de vice ; la possession est viciée par violence lorsque le possesseur s'approprie de la chose par la force et par menaces.
- Une possession publique : une possession doit être exercée aux vues et sus de tout le monde ; qu'elle soit manifestée par des actes apparents.
- Une possession non équivoque : l'équivoque est un vice qui touche l'un des deux éléments de la possession qui est l'élément intentionnel ; que la personne agit comme étant le véritable propriétaire du bien : l'animus. L'équivoque c'est l'ambigüité dans l'exercice de la possession qui laisse supposer que la possession pourrait être exercée à un titre autre que celui de propriétaire.

Ainsi, bien qu'il s'agit d'un fait, non un droit, la possession joue un rôle probatoire en ce qu'elle fait présumer que celui qui exerce le droit en est le titulaire légitime, mais aussi acquisitif, en permettant l'acquisition immédiate ou différée du droit exercé.

[437] William Dross, *Op. cit.*

[438] Le mot *corpus* présente le défaut de renvoyer à une corporéité qui n'est pas de l'essence de la possession (ce qui a pu conduire certains auteurs à proposer de l'abandonner au profit de la notion de pouvoir de fait : *A. Pélissier, cité supra n° 16, passim).*

[439] C. Aubry et C. Rau, *op. cit., § 177, p. 106.*

droit. C'est le fait d'avoir matériellement un bien en son pouvoir et d'être à même d'accomplir sur ce bien des actes matériels.

999. Si nous nous limitons à cette approche du *corpus* qui fait prévaloir l'aspect matériel, les actes électroniques n'auraient plus lieu d'exister car il faut toujours des actes d'usage concret d'une chose corporelle ; que le *corpus* est conçu comme un pouvoir physique sur la chose.

1000. La Cour de cassation[440] exclut toujours que nous puissions acquérir par prescription des biens immatériels ; au moins le juge est libre de décider, en l'absence d'actes matériels, que le corpus n'est pas suffisamment caractérisé[441].

1001. Toutes ces suppositions n'existent pas dans un environnement informatique. En conséquence, cette approche interdit clairement tout *corpus* et donc toute possession, portant sur des choses non matérielles, voire incorporelles ou électroniques.

1002. Par conséquent, la possession devient un instrument figé, inapte à saisir l'évolution fondamentale du droit des biens vers l'immatériel. Une conclusion qui incite à chercher une solution plus concrète pour admettre les 'documents transférables électroniques' dans la notion de la possession.

1003. Avec le corpus, il y a la notion de *l'animus ;* étant une donnée essentielle de la possession, l'*animus* révèle l'intention de celui qui possède d'agir comme étant le véritable titulaire du droit. C'est l'élément subjectif et intentionnel de la possession qui permet de savoir quel est exactement le droit exercé par le possesseur[442]. Ainsi pour établir l'*animus*, il faut examiner la volonté de celui qui accomplit les actes d'emprise sur la chose afin de le caractériser.

---

[440] Est cassé l'arrêt ayant admis la prescription acquisitive "sans relever d'actes de possession accomplis à titre de propriétaire" *: Cass. 3e civ., 25 févr. 1998, n° 96-15.045 : JurisData n° 1998-000834 ; Bull. civ. 1998, III, n° 48 ;* Defrénois *1998, art. 36828, p. 811,* obs. Ch. Atias. - *Cass. 3e civ., 27 janv. 1999, n° 96-18.436. - Cass. 3e civ., 1er avr. 2003, n° 01-03.941: JurisData n° 2003-018679.*

[441] Le juge reste libre de décider que le *corpus* n'est pas suffisamment caractérisé, notamment en l'absence d'actes matériels de jouissance. *Bull. civ. 2000, III, n° 159 ; D. 2000, inf. rap. p. 262.* Voir aussi *JCl. Civil Code, Art. 2276 et 2277 ou Notarial Répertoire, V° Prescription, fasc. 70*.

[442] William Dross, *Op. cit.*, n° 38 s.

1004. En règle générale, il y a une présomption simple de la possession (voire la présomption de l'*animus domini*) énoncée à l'article 2256 du Code Civil[443] qui édicte une présomption aux termes de laquelle *"on est toujours présumé posséder pour soi, et à titre de propriétaire (...)"*. Cette présomption simple de la possession qui fait que l'*animus* ne pose guère de problème en droit des biens, et qu'il incombe à la personne qui conteste la possession d'apporter la preuve de l'absence de l'*animus*[444].

1005. Le plus souvent, la nature de l'*animus* n'est pas contestée par les parties litigantes, et les juges considèrent *a priori* que les actes d'emprise exercés sur la chose, qu'ils soient matériels ou juridiques, le sont avec une âme de propriétaire.

1006. Le terme *animus domini* signifie l'intention de se comporter comme maitre ; ainsi il s'induit naturellement du *corpus* : les actes matériels sont le reflet de la volonté de celui qui les accomplit de se comporter en maître de la chose. Il en résulte que les juges n'ont pas à caractériser l'élément intentionnel de la possession, lequel est censé exister[445] et que c'est au revendicateur qu'il appartient de combattre la présomption[446].

1007. Pourtant, il est possible que les faits de possession, quoi qu'ils soient des actes matériels ou juridiques, soient insuffisants à caractériser un véritable *animus domini* en faveur de leur auteur. En d'autres termes, les actes accomplis sur la chose ne correspondent pas à ceux qu'aurait effectués un véritable propriétaire. Dans ce cas, la présomption édictée par l'article 2256 n'est plus fondée et la solution adoptée par les juges consiste à disqualifier entièrement la possession puisque l'*animus domini* n'est pas vraisemblable, il ne saurait y avoir de possession[447].

---

[443] Code Civil, version consolidée au 18 février 2015.
[444] William Dross, *Op. cit.*, n° 56 s.
[445] *Cass. 1er civ., 21 déc. 1964 : Bull. civ. 1964, I, n° 589. - Cass. 3e civ., 8 mai 1969 : Bull. civ. 1969, III, n° 371.*
[446] *Cass. 1er civ., 7 févr. 1962 : Bull. civ. 1962, I, n° 91. Dans ce sens,* le fait d'avoir pris certaines terres à bail n'interdit pas en principe au fermier de bénéficier de la présomption édictée par l'article 2256 à propos de parcelles non comprises dans le bail *(CA Caen, 26 mai 1998, n° 9601948 : JurisData n° 1998-045926)*
[447] *Cass. 1er civ., 25 févr. 1963 : Bull. civ. 1963, I, n° 119. - Cass. 3e civ., 18 mars 1970 : Bull. civ. 1970, III, n° 219 :* ne sont pas des actes de jouissance suffisants l'édification de constructions précaires. Ainsi lorsque les actes matériels accomplis par celui qui se prétend propriétaire n'ont pas une importance telle qu'ils traduisent l'exercice factuel d'un droit de propriété, la possession ne sera pas établie faute de corpus suffisant.

1008. Nous nous interrogeons ici sur l'applicabilité de la présomption d'‘*animus domini*’ sur les documents électroniques. Lorsqu'un porteur d'un document transférable électronique veut montrer la possession du document, doit il y avoir certains actes accomplis sur le document électronique qui ferait de lui un véritable propriétaire vis-à-vis des tiers ?

1009. Malheureusement, au lieu de nous aider à assimiler les documents papier et les documents électronique, la notion de la possession dans ces deux composants ‘animus’ et ‘corpus’ nous éloigne d'avantage de la reconnaissance du document électronique, car ni l'animus ni le corpus, tels qu'ils sont définis, ne peuvent exister dans un environnement électronique.

1010. Alors la seule solution pour transférer la notion de la possession en matière de document électronique est de trouver un "équivalent fonctionnel" à la possession qui corresponde à la nature particulière de l'environnent électronique que pourrait revêtir un ‘document transférable électronique’.

1011. Ainsi il convient d'établir une norme générale et souple capable de satisfaire l'ensemble des fonctions de la possession du document papier pour l'appliquer au document électronique.

II. La dématérialisation de la possession : une voie inefficace

1012. En droit des biens, le législateur avait l'intention d'aller plus loin avec la notion de la possession, et d'étendre la notion aux cas de figure dans lesquels le propriétaire n'est pas en mesure de posséder matériellement le bien[448].

1013. Nous avons présenté dessus les deux composantes de la possession: le *corpus* et l'*animus*. Le *corpus* comme étant l'élément matériel, associé à l'*animus domini*, constitue la possession et consiste dans l'accomplissement, sur la chose possédée, d'actes matériels comparables à ceux d'un propriétaire : actes d'usage, d'exploitation, de jouissance.

[448] William Dross, *Op. cit.*, n° 33 à 35.

1014. Toutefois, cette définition est imprégnée du droit romain qui limite la notion de la possession aux seuls actes matériels. C'est que cette définition étroite ne semble prendre en compte que le *corpus* appliqué aux seuls actes matériels adossés à la propriété (*possessio rei*), en excluant les actes juridiques possessoires (*possessio juris*), alors que l'acte de jouissance est bien sur caractérisé par la passation d'actes juridiques. Là nous évoquons les actes *possessio juris*. Ces derniers sont nécessaires à la circulation des choses, objets de la possession.

1015. Il s'agit ici d'actes juridiques qui peuvent avoir pour objet de conférer à un tiers une mainmise temporaire sur le bien, une mainmise lui permettant soit de le détenir de manière exclusive, soit d'en jouir concrètement pendant le laps de temps prévu au contrat.

1016. Dans ce cas, la préhension du bien ou son usage, qui caractérisent le *corpus*, ne seront pas le fait de l'auteur de l'acte mais du tiers. Il y a là usufruit concédé au tiers, droit réel, ou encore un contrat lui accordant des droits personnels et lui permettre la jouissance de la chose (i.e. contrat de prêt, de louage).

1017. Pour autant, ce tiers n'a pas l'*animus* d'un propriétaire puisqu'il n'a de maîtrise de la chose que précaire, l'acte fondant cette maîtrise l'obligeant à restitution. En revanche, cet *animus* existe pleinement chez l'auteur de l'acte : en concluant un contrat conférant à autrui le droit de détenir ou d'user de la chose, l'auteur de l'acte s'en considère comme maître. Le tiers use de la chose pour le compte de l'auteur de l'acte, lequel possède alors *corpore alieno*, par l'intermédiaire d'autrui.

1018. Ainsi le possesseur peut être conduit à se séparer matériellement de son bien au profit d'un autre. Il détiendra par autrui et possédera *corpore alieno*. C'est notamment le cas en droit des marques. Si le titulaire de la marque n'exploite pas mais qu'il confère son exploitation à un tiers, il n'encourt pas la sanction de déchéance pour inexploitation.

1019. Il est, certes, incontestable qu'en l'occurrence, le *corpus* existe pour le possesseur *corpore alieno*. Toutefois, à partir du moment où l'emprise matérielle sur la chose par le possesseur n'est pas directe, mais indirecte, la technique de la possession *corpore alieno,* qui sous-tend ce mécanisme, participe donc de la dématérialisation de la possession.

1020. La dématérialisation du *corpus* se décline en deux temps. D'une part, le possesseur *corpore alieno* réalise des actes juridiques qui relèvent des prérogatives caractéristiques du droit réel qu'il possède. Ensuite, celui par qui le possesseur *corpore alieno* détient la chose a une emprise matérielle sur la chose pour le compte de ce dernier.

1021. La loi a fait référence à la théorie de la possession '*corpore alieno*' dans le texte de l'article 2255 du Code civil lorsqu'il définit la possession comme "*la détention ou la jouissance d'une chose ou d'un droit que nous tenons ou que nous exerçons par nous-mêmes, ou par un autre qui la tient ou qui l'exerce en notre nom*". *Ainsi* le législateur français admet une possession pour autrui lorsqu'il existe une dualité de détention d'une chose ou d'exercice d'un droit par le possesseur ou par un autre pour lui.

1022. La jurisprudence en a aussi fait une bonne illustration de la théorie de la possession *corpore alieno.* Nous évoquons la décision de la Cour de Cassation en date de 18 décembre 2002[449] qui est très importante dans la mesure où elle enrichit la théorie de la possession *corpore alieno.*

1023. Selon l'arrêt attaqué (Papeete, 11 avril 2001) que par contrat en date du 16 mars 1990, la Société de banque occidentale (SDBO), aux droits de laquelle se trouve la société CDR créances, a consenti un prêt à la Société hôtelière internationale de Polynésie (SHIP), destiné à financer l'acquisition de trois ensembles hôteliers ; qu'en garantie, la société SHIP a consenti sur les biens acquis, avec la société Tapati, propriétaire du terrain sur lequel a été construit un des trois hôtels, une antichrèse inscrite le 22 août 1990 ; qu'il a été convenu que la

[449] Cass. 3e civ., 18 déc. 2002, *n° 01-12.143 : JurisData n° 2002-017037 ; Bull. civ. 2002, III, n° 261 ; RTD civ. 2003, p. 319,* obs. Th. Revet *; RTD civ. 2003, p. 327,* obs. P. Crocq.

société SHIP conserverait la jouissance des biens donnés en garantie, moyennant le versement, pendant douze années, d'une indemnité d'occupation ; que la société SHIP a cessé ses règlements en 1994 et que la société CDR créances a déclaré sa créance au passif des sociétés SHIP et Tapati, mises en redressement judiciaire le 6 juillet 1998.

1024. Pour déclarer les antichrèses éteintes, la cour d'appel a relevé que la société SHIP avait cessé tout règlement de l'indemnité d'occupation à compter de novembre 1994 et retenu que la société CDR créances, jusqu'au dépôt de sa déclaration de créance, le 16 octobre 1998, n'avait pris aucune initiative concrète soit pour rompre la convention d'occupation et confier l'exploitation à un tiers afin de maintenir sa possession juridique, soit pour prendre possession matériellement des immeubles afin d'exercer son droit de rétention et que le fait pour l'antichrésiste de n'entreprendre aucun acte positif destiné à marquer sa volonté de garder la possession matérielle ou juridique des biens nantis avait eu pour conséquence de faire disparaître la condition essentielle de la validité de l'antichrèse, à savoir la dépossession du constituant ; que d'après le juge de la Cour de cassation, en statuant ainsi, alors que la société SHIP, qui avait cessé de régler les indemnités d'occupation, continuait cependant à posséder pour le compte de l'antichrésiste et que l'absence d'action de ce dernier contre elle n'avait pas mis fin à cette possession, la cour d'appel a violé les textes de l'article 2228 du code civil, ainsi que les articles 2085, 2086, 2231 et 2240 du code civil.

1025. Alors, selon cet arrêt le juge de cassation a infirmé la décision des juges du fond, en justifiant sa décision de cassation sur le simple rappel de l'article 2228, sans pour autant ressortir une définition précise de la possession *corpore alieno*. Bien que ni la jurisprudence ni le Code Civil n'aient pas prévu une définition précise de la notion de la possession *corpore alieno*, on trouve que pour les auteurs contemporains, dans leur précieux ouvrage consacré aux Locutions latines du droit français, les professeurs Roland et Boyer[450] ont parvenu à définir la notion de possession *corpore alieno* comme un « *mode d'acquérir ou de conserver la possession par l'intermédiaire d'autrui. Au rebours de l'élément*

[450] H. Roland et L. Boyer, *Adages du droit français* : *Litec*, 4e éd. 1999.

intentionnel (animus) qui est requis en la personne même qui doit posséder, l'élément matériel (corpus) est susceptible d'être exercé par un tiers ..., celui qui cesse de posséder matériellement sa chose ne perd pas la possession lorsque les faits constitutifs de cette possession sont l'œuvre d'autrui » (exemples nombreux en droit de la propriété industrielle : brevet et marque).

1026. Il en reste de savoir si la possession *corpore alieno* est une théorie appropriée pour s'appliquer au document électronique. Cette théorie de la possession *corpore alieno* est très importante dans la mesure où elle ouvre la voie vers la reconnaissance des documents électroniques puisqu'elle partage un élément commun avec ces derniers ; celui du détachement de la chose et ainsi de rendre acceptable la dématérialisation de la possession.

1027. Bien que la dématérialisation de la possession soit reconnue grâce à la possession *corpore alieno*, nous avons tout de même besoin de trouver une norme générale qui soit un équivalent fonctionnel de la possession pour admettre le transfert du 'document transférable électronique'.

1028. **– Conclusion intermédiaire** – Après avoir présenté les éléments constitutifs de la possession (l'*animus* et le *corpus*), puis la théorie de *corpore alieno* qui rapproche le 'document transférable électronique' en droit des biens, il convient de trouver un critère équivalent fonctionnel adapté à l'environnement informatique et constitue un substitut à la notion de la possession.

PARAGRAPHE II – LE "CONTROLE" SUBSTITUT DE LA POSSESSION

1029. Afin de mieux cerner la question de l'équivalence de la possession dans un environnement électronique, il nous convient de cibler le droit des contrats et le droit des obligations[451].

1030. Lorsqu'il s'agit d'un document papier, c'est la possession de l'unique document, consignant les droits et les obligations, qui est généralement exigée pour qu'une personne ait le droit de s'en prévaloir. Et la personne légalement en possession du document est généralement appelée le 'porteur', désignant la personne qui a le droit de se prévaloir du document.

1031. Les droits sur la livraison de marchandises représentés par des documents titres dépendent originairement et par défaut de la possession matérielle d'un document papier unique ; ce qui est le cas par exemple en matière du connaissement et du récépissé d'entrepôt.

1032. De même, les droits au paiement d'une somme d'argent représentés par des instruments transférables dépendent aussi en règle générale de la possession matérielle d'un document papier unique. C'est le cas du billet à ordre, la lettre de change et les chèques.

1033. Comme ces documents formant titre pouvaient produire des effets à l'égard des tiers, les systèmes papier renvoyaient à des notions telles que la "possession" et la qualité de "porteur".

1034. La difficulté consistait à transposer ces notions dans un environnement électronique en définissant des équivalents pouvant produire les mêmes résultats que des documents papier.

[451] Friedrich Karl Von Savigny, *Traité de la possession en droit romain*, traduit de l'allemand par CH. Faivre D'Audelange, *Imprimerie De Cosse et Gaultier-Laguionie*. 6e édition. 1841. p.29.

1035. Pour les ‘documents transférables électroniques’, l’exigence de garantie de singularité s’accompagne de celle de possession matérielle du document papier qui représente l’obligation. C’est la possession de l’unique document consignant les droits et les obligations qui est généralement exigée pour qu’une personne ait le droit de s’en prévaloir.

1036. Le papier avait été choisi comme support pour les documents formant titre en raison de ses caractéristiques qui permettent par exemple d’enregistrer et de transmettre facilement ces documents. Ces traits caractéristiques du support papier doivent être pris en compte pour designer l’équivalent fonctionnel que nous pouvons utiliser pour un document électronique.

1037. Ainsi dans le cadre de cette approche fondée sur l'équivalence fonctionnelle, il serait peut-être préférable d’adopter une norme qui est à la fois large et souple pour satisfaire l’ensemble des fonctions du document papier dans un environnement électronique, plutôt que de mettre en œuvre des normes distinctes visant à remplir chacune de ses fonctions.

1038. La désignation d’une norme souple doit bien répondre à la nature particulière de l’environnement électronique qui est assujetti au développement technologique ayant un rythme rapide et très varié.

1039. Pourtant cela n’empêche pas que la possession est un critère important à concilier avec le monde informatique, non pas parce que les documents papier tangibles ont en soi de la valeur, mais aussi parce qu’une seule personne peut être en possession d’un objet tangible à un moment donné.

1040. Dans la plupart des modèles juridiques régissant les ‘documents transférables électronique’, la notion de “contrôle” d’un document électronique est utilisée en tant qu’équivalent fonctionnel de la possession. Cela signifie que la personne qui exerce le contrôle du ‘document transférable électronique’ est considérée comme le porteur habilité à s’en prévaloir.

1041. Lorsque le contrôle d’un tel document se substitue à la possession du document papier transférable, le transfert du contrôle se substitue à la remise du

‘document transférable électronique’, tout comme le transfert de possession (et l’endossement s’il y a lieu) se substitue à la remise du document papier transférable.

1042. **Si** le contrôle sert de substitut à la possession, il doit exister une méthode pour identifier la partie qui exerce actuellement le contrôle d’un ‘document transférable électronique’ donné. Pour ce faire, nous pouvons soit attester l’identité de la personne concernée dans l’exemplaire faisant foi, soit associer ce dernier à une méthode permettant de retrouver l’identité de la personne (par exemple un registre), de manière à ce qu’une personne qui consulte cet exemplaire puisse constater l’existence du contrôle et avoir accès aux preuves correspondantes.

1043. De manière générale, la plupart des législations en vigueur, telles que dans le système juridique français, anglo-saxon et américain, considèrent qu’il n’est pas nécessaire qu’un ‘document transférable électronique’ possède des caractéristiques intrinsèques qui le rendent réellement “unique” en ceci qu’il ne peut exister de copies identiques.

1044. Elles s’attachent plutôt à établir l’équivalence fonctionnelle de l’unicité par le biais d’exigences visant: 1) à assurer l’intégrité et la disponibilité d’un exemplaire au moins du ‘document transférable électronique’ en désignant un exemplaire qui fait foi (c’est-à-dire préciser et déterminer les termes du document transférable électronique), et 2) à identifier le propriétaire ou porteur (c’est-à-dire la personne qui exerce le contrôle) du document transférable électronique. Dans ce contexte, le critère de “contrôle” est en général défini d’une manière qui met l’accent sur l’identité de la personne habilitée à se prévaloir des droits incorporés dans le ‘document transférable électronique’.

1045. Par exemple, en vertu de la loi des États-Unis relative aux signatures électroniques dans le commerce national et international[452], une personne est

[452] Titre 15 de l’*United States Code Annotated « Commerce and Trade »*, chap. 96 *« Electronic Signatures in Global and National Commerce »*, voir par. 7001 et suivants. [En ligne : https://www.law.cornell.edu/uscode/text/15/chapter-96/subchapter-I].

réputée exercer le contrôle d'un 'document transférable électronique' si le système utilisé pour attester le transfert de droits sur un document transférable établit de façon fiable que cette personne est celle en faveur de laquelle le document transférable a été bien émis ou transféré.

1046. L'idée est fondée sur l'identification d'un équivalent fonctionnel à la possession, que le texte de la loi susmentionnée désigne par les termes de "contrôle" ou de "contrôle exclusif" du document, à partir duquel nous déterminons le mécanisme ou le protocole de transfert du document électronique et des droits qui y sont incorporés.

1047. Dans cette méthode, le transfert du document nécessite le transfert du contrôle sur celui-ci, et pour se prévaloir des droits conçus dans le document, la preuve de ce contrôle est nécessaire. Pour comprendre ce que peut représenter le contrôle d'un document, il faut bien retenir que, dans des opérations engagées et exécutées par des moyens électroniques, tout échange ou transfert de biens meubles incorporels, tels que des documents transférables électroniques, repose sur l'échange d'informations entre les parties par le biais du réseau de communications électroniques. Cela implique que le contrôle se fonde uniquement sur l'échange d'informations qui se présenteront le plus souvent sous forme écrite. Le contrôle joue le rôle d'un indicateur fiable de propriété ; il remplit ainsi les fonctions que nous associons, dans un environnement papier, aux informations écrites sur le document (comme l'identification du titulaire à travers des exigences formelles telles que l'endossement) et celles qu'on attribue à la possession, et notamment en raison des systèmes de cryptologie mis en place.

1048. L'essentiel à retenir selon cette loi américaine sur la signature électronique est de démontrer que le système mis en place établit de façon fiable l'identité de la personne habilitée à recevoir le paiement d'une somme d'argent ou la livraison de marchandises, que ce soit à l'aide d'un registre tenu par un tiers ou d'autres moyens de protection technologiques.

1049. L'article 16 de la Loi uniforme sur les opérations électroniques aux Etats Unis[453] régit les conditions dans lesquelles il est possible d'émettre des 'documents transférables électroniques' ayant les mêmes buts et les mêmes effets que des documents papier. Il prévoit d'ailleurs sur le critère de contrôle qu' « une personne a le contrôle d'un document transférable électronique si le système utilisé, démontre le transfert d'intérêts en droit dans le document transférable, et établit de façon fiable que cette personne est celle à laquelle le document transférable a été délivré ou transféré » (article 16-b)[454].

1050. Les dispositions de cette loi uniforme américaine s'appliquent en particulier aux billets à ordre et aux titres représentatifs de marchandises. Il y a aussi le Code de commerce uniforme des Etats Unis d'Amérique[455], qui régit, dans son article 7, les titres représentatifs de marchandises émis sous forme négociable et par voie électronique.

1051. D'autres textes ont la même approche et ont adopté la notion de contrôle comme critère prépondérant d'équivalence par rapport à la possession. Parmi ces textes, il y a la Convention des Nations Unies sur le contrat de transport international de marchandises de 2008 (les Règles de Rotterdam)[456]. Cette Convention a pour objectif d'établir un régime juridique uniforme et moderne pour régir les droits et obligations des chargeurs, transporteurs et destinataires en vertu d'un contrat de transport de porte à porte comprenant une étape maritime internationale. Ces règles de Rotterdam de 2008 tiennent compte de nombreuses nouveautés technologiques et commerciales qu'à connues le transport maritime depuis l'adoption de ces conventions, tel le développement des documents électroniques de transport.

---

[453] *Uniform Electronic Transactions Act (UETA)* in 1999 (la Loi uniforme sur les opérations électroniques de 1999) (UETA). . [En ligne : http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf].

[454] Section 16 (b) : "*A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred".*

[455] Le Code de commerce uniforme des Etats-Unis d'Amérique élaboré par l'American Law Institute et la *National Conference of of Commissionaires* on *Uniform State Laws*. compte-rendu ; n°4 ; vol.15, p. 733, Revue internationales de Droit Comparé.

[456] Convention des Nations Unies sur le contrat de transport international de marchandises effectué entièrement. ou partiellement par mer (les "Règles de Rotterdam") (New York, 2008), *Ed. Nations Unies*, juillet 2014. [En ligne : http://www.uncitral.org/pdf/french/texts/transport/Rotterdam_Rules/Rotterdam-Rules-F.pdf].

1052. La Convention traite dans son chapitre 3 les documents électroniques de transport ; d'après l'article 8 de la Convention, peut être consignée dans un document électronique de transport tout ce qui doit figurer dans un document de transport en vertu de la convention. La Convention reconnait dans le deuxième alinéa du même article que « *l'émission, le contrôle exclusif ou le transfert d'un document électronique de transport a le même effet que l'émission, la possession ou le transfert d'un document de transport* ». Ainsi la Convention autorise de produire des documents électroniques pour toutes les étapes d'exécution d'une opération de transport maritime internationale, le critère de contrôle est accepté pour se substituer à la possession lorsque nous envisageons un document électronique. (article 8 - b).

1053. Ces textes susmentionnés supposent que les parties se prêtant à l'utilisation d'un 'document transférable électronique' conviennent du système et de la technologie à employer pour son émission et son utilisation. Dans ce contexte, un facteur essentiel pour la reconnaissance de la validité de l'émission et du transfert d'un 'document transférable électronique' est celui de la technologie nécessaire au transfert, son degré de disponibilité sur le marché, l'architecture et le protocole ou mécanisme qui l'emportent en pratique et le degré de fiabilité qu'elle atteint dans la réalisation de la fonction indiquée, à savoir, l'identification, en toutes circonstances, du titulaire du document transférable (*supra* partie I).

1054. Enfin, il convient de mentionner qu'en l'absence d'unicité technique des documents électroniques, l'approche du contrôle peut aussi aider à satisfaire l'exigence de singularité du document papier transférable. En prévoyant une procédure pour désigner l'identité de la personne qui exerce le contrôle du 'document transférable électronique' (ainsi qu'une procédure visant à déterminer sur "quoi" le porteur détient un intérêt), nous éliminons les craintes quant à l'existence d'exemplaires multiples du document, car la propriété (c'est-à-dire le statut de porteur) n'est pas déterminée par la possession d'un exemplaire du document même, et le transfert n'implique ni modification ni endossement desdits exemplaires.

1055. – Conclusion intermédiaire – En traitant les différents critères de la possession, nous sommes parvenus à la notion de contrôle comme équivalent fonctionnel pour les documents électroniques. Ainsi une autre question se pose : Adopter un régime juridique pour régir un 'document transférable électronique' fait surgir l'épreuve de pouvoir identifier la personne en possession du document représentant l'obligation, soit le créancier ou le bénéficiaire de la valeur qu'il représente.

SECTION 2 – IDENTIFICATION DU PORTEUR DU 'DOCUMENT TRANSFÉRABLE ÉLECTRONIQUE'

1056. Il est nécessaire d'identifier de manière fiable les parties au 'document transférable électronique', comme l'émetteur original et l'auteur du transfert. Concrétisant la problématique de la présente section, il s'agit de savoir s'il existe des moyens fiables pour nous aider à identifier les personnes dans une transaction impliquant un 'document transférable électronique'.

1057. Nous envisageons ainsi les différents modèles pour identifier la personne qui exerce le contrôle, et comment archiver les documents électroniques via *Records management (Paragraphe I).* Ensuite, nous présentons la conservation pérenne du document électronique (Paragraphe II)

PARAGRAPHE I – CONSERVATION FIABLE DU DOCUMENT ÉLECTRONIQUE

1058. Nous avons traité précédemment, dans le chapitre 2 de la première partie sur le droit de la preuve et la signature électronique, les dispositions de la loi qui répondent à la question de la fiabilité des documents électroniques en proposant des méthodes cohérentes et capables d'identifier les personnes signataires.

1059. Bien que le porteur soit la personne habilitée à se prévaloir du 'document transférable électronique', son identité peut ne pas être consignée dans le document transférable lui-même, et il peut changer lorsque le document est transféré d'une personne à une autre.

1060. Aussi un mécanisme doit-il être mis en place pour pouvoir identifier la personne qui, à un moment donné, est considérée comme étant le porteur. Dans un environnement papier, la personne en possession d'un document transférable unique est présumée être le porteur. Par contre, ce n'est pas aussi simple dans un environnement électronique, où il est nécessaire de remplacer le concept de possession par son équivalent fonctionnel 'le contrôle', un mécanisme doit ainsi être mis en place pour établir l'identité de cette personne présumée 'porteur'.

I. Principales approches établissant l'identité de la personne exerçant le contrôle

1061. Présentons les principales approches permettant d'établir l'identité de la personne en faveur de laquelle le 'document transférable électronique' est émis ou transféré (c'est-à-dire la personne exerçant le contrôle)

A. <u>Le modèle du support.</u>

1062. Selon cette approche, l'identité de la personne qui exerce le contrôle du 'document transférable électronique' (le porteur) figure dans le document électronique proprement dit, et les changements de propriété (par exemple, cessions ou transfert par endossement) sont directement consignés dans le 'document transférable électronique'[457].

1063. Ici il convient de s'assurer que le système est en mesure d'exercer un contrôle régulier et scrupuleux sur le document électronique proprement dit, et sur le processus de transfert du contrôle, ainsi que le pouvoir de tracer le titulaire véritable suite à un transfert ou cession.

[457] *Questions juridiques liées à l'utilisation des documents transférables électroniques*, '*A/CN.9/WG.IV/WP.115*', *Op. cit.*,p.14 et s.

1064. En d'autres termes, tout comme pour les documents transférables sur support papier, il peut être nécessaire de mettre en place des garanties d'ordre technique ou sécuritaire pour faire en sorte qu'il n'existera qu'"un seul exemplaire faisant foi", qui ne pourra être ni copié ni modifié et auquel nous pouvons se référer pour déterminer l'identité du titulaire ainsi que les termes du 'document transférable électronique' proprement dit. Nous avons traité la notion de l'exemplaire faisant foi au début de la deuxième partie[458].

1065. Donc l'efficacité du présent modèle se mesure par rapport à sa capacité de pouvoir démontrer qu'il est impossible pour qui que ce soit d'altérer ou de manipuler le document électronique sans que cette personne soit identifiée sur le système.

1066. Il est d'ailleurs important que le modèle utilisé dispose de certaines mesures de sécurité visant à la restriction de l'accès aux documents électroniques consignés sur les ordinateurs. Ces mesures peuvent être mise en place par divers moyens, notamment l'utilisation de mots de passe ou l'authentification biométrique pour entrer dans le système[459]. Il s'agit d'une technique de sécurité intrinsèque au document.

B. Le modèle du registre.

1067. Selon le modèle du registre, l'identité[460] du titulaire du 'document transférable électronique' est consignée dans un registre distinct tenu par un tiers indépendant ; ce dernier est considéré comme un dépositaire et garant de la sécurité.

---

[458] Voir *supra*, n°941 s.

[459] Le projet *InterPARES* est principalement financé par le Conseil de recherches en sciences humaines du Canada ainsi que par la *National Historical Publications and Records Commission* et la *National Science Foundation* des États-Unis. Les fonds de contrepartie sont fournis par le *Hampton Fund Research Grant*, le Vice Président *Research Development Fund*, le doyen des Arts et la *School of Library, Archival and Information Studies* de l'Université de la Colombie-Britannique. [En ligne : http://www.interpares.org/ip2/display_file.cfm?doc=ip2_preserver_guidelines_booklet_french.pdf].

[460] Voir *supra* n°505.

1068. Afin d'établir de manière fiable l'identité du titulaire du 'document transférable électronique' il convient d'exercer un contrôle qui s'applique par le registre. Ce modèle du registre joue un rôle prépondérant pour identifier le titulaire/porteur du document électronique.

1069. Dans cette hypothèse, l'unicité de l'exemplaire du 'document transférable électronique' n'est plus un critère déterminant, voire même moins importante, aussi longtemps qu'il existe un moyen de vérifier l'intégrité du document en accédant un registre sécurisé ayant un contrôle fiable.

1070. Dans ce modèle du registre le 'document transférable électronique' ne fait que mentionner le registre où nous pouvons trouver l'identité de la personne exerçant le contrôle, qui ne change pas au fil du temps, ni en cas de cession.

1071. Concernant les exemplaires du 'document transférable électronique', la principale préoccupation est de pouvoir disposer d'un mécanisme permettant de déterminer si un exemplaire donné est exact, que son intégrité est intacte, de la sorte que toute personne consultant l'exemplaire, via le registre, puisse repérer le titulaire du titre, à ce point que le véritable titulaire identifié dans le registre puisse se prévaloir dudit exemplaire[461].

1072. Ici nous soulignons que la notion de contrôle associée à des préoccupations de sécurité privilégie essentiellement le registre, de préférence au document transférable proprement dit.

1073. La méthode du 'Registre' permet à la fois à l'exemplaire spécifique qui constitue l'"exemplaire faisant foi" et le système informatique dans lequel il est stocké de changer avec le temps, sans soulever le moindre souci par rapport à la fiabilité des informations sur le registre.

1074. Afin d'y parvenir, il est fréquent de se servir d'un registre pour localiser l'endroit où l'exemplaire faisant foi est stocké, et/ou de conserver une empreinte

[461] *Questions juridiques liées à l'utilisation des documents transférables électroniques*, *Op. cit.*, p.16 et s.

digitale numérique (par exemple, valeur de hachage ou signature électronique) de l'exemplaire faisant foi pour que nous puissions facilement déterminer si l'intégrité de l'exemplaire conservé par le porteur, ou en son nom, est intacte et correspond à l'original[462].

1075. Cette approche de registre, permet de créer, de stocker et de transférer le 'document transférable électronique' dans toute une gamme de systèmes d'information courants, certaines informations étant transmises à un registre central où elles sont enregistrées ; et que l'accès au registre pouvait être contrôlé et obéit à l'acceptation de dispositions contractuelles[463].

1076. Par ailleurs, l'exemplaire faisant foi du 'document transférable électronique' n'est pas nécessairement stocké dans le registre ; il est possible de vérifier l'exactitude de tout exemplaire en consultant celui-ci. Dans certains systèmes, pour procurer de la crédibilité aux informations transmises, le registre contient l'exemplaire faisant foi et mentionne l'identité de la personne qui en exerce le contrôle.

1077. Dans d'autres systèmes, le registre contient simplement la signature numérique de l'exemplaire faisant foi, qui est ainsi accessible pour vérifier l'intégrité de tout exemplaire dont la personne exerçant le contrôle voudra à terme se prévaloir.

1078. Les textes législatifs français ne définissent pas encore les modalités du registre ; pourtant ils imposent l'archivage de certains documents numériques, ce qui suppose une entité tel le registre, qui est indépendant des opérateurs.

1079. Le registre est ce tiers de confiance dont nous avons parlé tout au long de la première partie ; ce dernier délivre les clés asymétriques (utilisées pour le chiffrement et le déchiffrement des documents électroniques) sous la forme du Prestataire de services de certification électronique (PSCE), tel est le cas du

[462] *Questions juridiques liées à l'utilisation des documents transférables électroniques , Op. cit.,* p.12 et s
[463] *Questions juridiques liées à l'utilisation des documents transférables électroniques*, *Op. cit.,* p.16 et s.

centre de certification issu de l'ANSSI[464]. Le registre peut aussi être le prestataire qualifiés[465] qui fournit les services de confiance aux usagers.

1080. D'ailleurs, selon l'article L. 134-2 du Code de la Consommation[466], concernant les contrats crées et conclus par voie électronique, le contractant professionnel s'engage à assurer la conservation de l'écrit qui le constate et en garantit à tout moment l'accès à son cocontractant si celui-ci en fait la demande.

1081. Dans un raisonnement par analogie du texte de l'art. L. 134-2 du Code de Consommation sur un 'document transférable électronique', nous retenons que dans le modèle de registre, un professionnel est le registre et le cocontractant est le titulaire du document (le porteur) ; par conséquent, le registre sera tenu responsable pour assurer une conservation pérenne du document électronique.

1082. Pour tout ce qui est protection des données à caractère personnel, nous renvoyons aux dispositions du règlement européen du 27 avril 2016, présentées dans la première partie[467].

C. Personne exerçant le contrôle, définie en tant que personne disposant d'un accès exclusif.

1083. Il s'agit ici de l'hypothèse dans lequel l'exemplaire faisant foi du 'document transférable électronique' est stocké dans un système informatique sécurisé et conçu à cet effet. Ce système de stockage est protégé par des mesures de contrôles de sécurité et d'accès appropriés qui permettent de définir la personne qui exerce le contrôle (qui est le porteur) comme l'unique personne

[464] Voir *Supra* n°609.
[465] Voir *Supra* n°691 s.
[466] Article L134-2 du Code de la consommation (Version consolidée au 1 juillet 2015) : '*Lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à un montant fixé par décret, le contractant professionnel assure la conservation de l'écrit qui le constate pendant un délai déterminé par ce même décret et en garantit à tout moment l'accès à son cocontractant si celui-ci en fait la demande*'. [En ligne : http://legifrance.gouv.fr/affichCode.do;jsessionid=029E443E781A7AB137CAF659B462AA5D.tpdila23v_1?cidTexte=LEGITEXT000006069565&dateTexte=20150720].
[467] Voir *supra* n°139 s.

ayant accès au ‘document transférable électronique’ en question. En pareil cas, le transfert du contrôle exige le transfert du moyen d’accès sécurisé exclusif, un support d’accès unique par exemple.

1084. Evidemment, nous pouvons concevoir d’autres approches qui utilisent la technologie pour identifier les personnes contractantes, la procédure ou l’agrément en lieu et place de l’unicité, et que si certaines lois autorisent ou exigent l’une ou plusieurs des approches évoquées ci-dessus, d’autres n’ont pas tranché la question, et que ni la Loi type sur le commerce électronique ni les Règles de Rotterdam ne précisent la méthode à utiliser pour garantir cette singularité; elles laissent les parties libres d’en convenir.

1085. **– Conclusion intermédiaire** – Ces différentes méthodes nous permettent d’identifier le porteur du document électronique pendant son exécution. Pourtant, lorsque le document électronique prend fin, il doit aussi être préservé pour un certain temps pour la preuve, c’est l’intérêt d’avoir un système d’archivage électronique.

II. L’archivage électronique et la fonction de ‘tiers archiveur’

1086. Nous avons envisagé jusqu'à présent les différents stades de création et d’exécution du ‘document transférable électronique’. Lorsque la transaction commerciale est terminée, il n’en reste pas moins que le document doit perdurer pendant une certaine période pour des raisons de preuve s’il apparait un litige. Nous présentons l’archivage électronique (A), pour introduire le métier de *record management* dans l’environnement informatique (B).

A. Contexte historique de l’archivage électronique

1087. L’archivage dans le sens où nous parlons aujourd’hui est le résultat d’une longue histoire pour parvenir à la phase actuelle dont nous témoignons aujourd’hui. Depuis toujours, le gonflement rapide de la « paperasse » dans le secteur public menace d’envahir les bureaux, couloirs, caves et greniers ; ce qui a poussé les administrations de repenser et réorganiser le traitement de leurs archives courantes.

1088. D'abord les administrations ont eu recours aux centres de pré-archivage pour désengorger les bureaux avant de pouvoir procéder, tout en respectant les délais de prescription légale pour chaque document, aux éliminations et au versement dans le dépôt d'archives. Cette étape de pré-archivage des documents marque la dernière phase dans leur cycle de vie lorsqu'ils deviennent de moins en moins utiles de point de vue administratif[468].

1089. Jusqu'au milieu du dernier siècle la définition d'archive se limitait aux documents d'intérêt historique de valeur permanente conservés dans les archives publiques. Puis grâce à la théorie des trois âges[469], le terme 'archive' se trouve étendu pour comprendre « *l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, dans l'exercice de leur activité, documents soit conservés par leur créateur ou leur successeurs pour leurs besoins propres, soit transmis à l'institution d'archives compétente en raison de leur valeur archivistique*. »[470]

1090. Cette notion d'archive est indépendante de la date des documents et de leur forme et support physique[471]. Cette définition générale découlant de la théorie classique « des trois âges » est mise à l'épreuve face à l'archivage électronique ; il n'est plus pertinent de parler de trois âges lorsque nous nous intéressons aux archives électroniques pour des raisons techniques : en effet si un document n'est pas pris en charge dès sa création, il sera extrêmement difficile d'évaluer son intégrité *a posteriori*[472]. En ce sens, la notion d'archivage intermédiaire[473] n'est plus pertinente.

---

[468] JOLY-PASSANT (E.), *Op. cit.*

[469] La théorie des trois âges est une notion fondamentale sur laquelle repose l'*archivistique* contemporaine, et qui fait passer tout *document* par trois périodes, en fonction de leur utilisation, courante, intermédiaire et définitive, caractérisées par la fréquence et le type d'utilisation qui en est faite. [En ligne : http://www.arcalys.com/archivage/definition-theorie-des-trois-ages/].

[470] Peter WALNE (ed.), Dictionary of Archival Terminology, English and French with Equivilents in Dutch, German, Italian, Russian and Spanish. K.G. Saur, Munchen-New York-London-Paris, 1984, 226 p. (ICA Handbooks Series. Volume 3).

[471] En ligne : http://www.avae-vvba.be/index.php?page=services&souspage=gestion&lang=fr.

[472] Article sur l'Archivage électronique à l'épreuve de la théorie des trois âges. [En ligne : https://archivesonline.wordpress.com/2010/08/30/larchivage-electronique-a-lepreuve-de-la-theorie-des-trois-ages/].

[473] Les archives intermédiaires sont définies comme des documents qui ont cessé d'être considérées comme des archives courantes et qui ne peuvent, en raison de leur intérêt et/ou des textes légaux et réglementaires

1091. D'ailleurs, malgré le fait que la loi ne prévoit pas une définition à l'archivage, la norme technique ISO 15489[474] est venue préciser que l'archivage consiste en un : « *système d'informations qui intègre les documents, les organise, les gère et les rend accessible a terme* ». D'après cette définition, l'archivage est un terme technique qui désigne toute méthode de gestion et d'organisation des archives. Les archives sont l'objet sur lequel porte l'archivage, la manière d'ordonner et de disposer de cet objet[475].

B. L'archivage électronique et le Records Management

1092. S'agissant d'un concept moderne associé à l'archivage, le 'Records Management' est la *fonction, exercée dans le cadre de la gestion administrative, de gérer avec économie et efficacité la création, la conservation, le tri et l'utilisation des documents*.

1093. Dans l'intérêt de développer la fonction de l'archive et faire face à l'inflation documentaire, l'intervention en amont pour simplifier et normaliser les procédures a fait naître la profession de '*Records Managers*' (Gestionnaires de Documents).

1094. Pourtant, la fonction de '*Record Management*' est distincte de celle des archivistes. Le *record management* est un métier qui attribue à la même personne la mission de créer le document et le contrôler. Or l'objectif du métier 'records management' est de faciliter le passage à l'ère de numérique et des archives dématérialisées[476].

1095. Ainsi la dématérialisation s'est avérée nécessaire du fait de l'utilisation grandissante des outils informatiques ; afin d'archiver des données notamment

---

(durées de conservation), faire l'objet d'élimination. [En ligne : http://www.ago-sa.fr/lexique/entry-11-archives-intermediaires.html].

[474] l'ISO 15489 constitue un guide pour l'organisation et la gestion des documents d'archives) des organismes, publics ou privés, pour le compte de clients internes ou externes. [En ligne : http://www.iso.org/iso/fr/catalogue_detail.htm?csnumber=31908].

[475] JOLY-PASSANT (E.), *Op. cit., p.*431 et s.

[476] Pour savoir plus sur la fonction de '' Records Manager'', veuillez consulter l'adresse suivante : http://www.lenouveleconomiste.fr/lesdossiers/la-fonction-de-records-manager-15723/.

volumineuses, il est désormais procédé à la dématérialisation de l'information, des données, dans la mesure où la majeure partie des documents est créée *ab initio* sous format numérique. C'est la rapidité de traitement des données et la facilité de communication de documents qui expliquent le développement de ce procédé.

1096. La fonction *Record Management* s'évolue d'avantage, désormais intitulée '*Information Management' ('Gestion de l'Information'),* ce qui est un terme plus approprié dans le nouveau contexte de l'environnement numérique[477].

1097. En principe, nous pouvons avoir deux types d'infrastructure de conservation pour les documents électroniques relevant des activités bancaires[478]:

1098. D'une part, lorsque la conservation est gérée par des infrastructures internes, l'ensemble de processus de conservation est placé sous le contrôle de la banque qui produit ou reçoit les documents à conserver/ à archiver. Cette solution apparait peu pratique car comme les documents conservés restent sous l'unique contrôle de la banque, il n'est pas certain que la banque pourra apporter toutes les garanties au document conservé, notamment si les documents conservés utilisent les technologies cryptographiques.

1099. D'autre part, ayant pour souci de garantir leur 'documents transférables électroniques', la banque fait recours à des professionnels ayant de l'expertise en matière de conservation des documents, appelés les 'tiers archiveurs'.

1100. Malgré l'importance croissante du rôle du 'tiers archiveur', particulièrement dans la société d'information, il est regrettable de ne pas avoir une définition ni du terme 'tiers archiveur', ni à sa fonction.

1101. La professeur Elisabeth JOLY PASSANT a attribué une définition générique au 'tiers archiveur' ; il s'agit d'*une entité désignée par des utilisateurs (personnes publiques ou privées) ou leur mandataire de recevoir, conserver et d'assurer la gestion des documents dont il a la charge. Ce tiers archiveur doit*

[477] En ligne : http://www.aiim.org/What-is-Information-Management.
[478] JOLY-PASSANT (E.), *Op. cit.,* p.490 s.

être capable de présenter des documents signés et reconnus comme tels, à tout moment, des années après leur date de mise en archive[479].

1102. Les tiers archiveurs sont donc un prestataire de service public ou privé. Les obligations principales dédiées à la mission du tiers archiveur peuvent être résumées dans l'ordre suivant[480]:

- utiliser un format des documents approprié et durable ;
- vérifier que les documents qu'il conserve portent une signature valide ;
- garantir la lisibilité et l'intelligibilité des documents mis en archive, ainsi que leur accessibilité. Ceci implique qu'il conserve tout élément logique ou physique lui permettant d'atteindre ce but ;
- procéder à la re-signature de manière régulière, avant que la technologie cryptographique utilisée initialement ne devienne vulnérable ;
- Enfin, pour maintenir l'intégrité des documents qu'il conserve et assurer l'identification de la personne dont ils émanent, le tiers archiveur devra employer tous moyens pour éviter la survenance de bugs ou la défaillance de son installation.

1103. **– Conclusion intermédiaire** – Nous constatons que les métiers du *record management* et le tiers archiveur sont importants pour conserver les documents électroniques. Pour les assister d'accomplir leur tache, il existe des matériels et des logiciels spécialisés dans le domaine de conservations de données informatiques.

[479] *Ibid*.
[480] JOLY-PASSANT (E.), *Op. cit.*, p.496 s.

PARAGRAPHE II : CONSERVATION PÉRENNE DU DOCUMENT ÉLECTRONIQUE

1104. La lisibilité des données électroniques doit être assurée à plus ou moins long terme : les supports de stockage, le matériel (hardware) et les logiciels (software) évoluent rapidement et se succèdent, si bien qu'il est difficile de lire des fichiers enregistrent sous des formats périmés ou sur des supports obsolètes ou altérés.

I. Aperçu historique du défi de la conservation des documents électronique dans le temps

1105. Remontons dans l'histoire, suite à la conquête de l'Angleterre, Guillaume le Conquérant ordonna d'évaluer et de recenser les biens de son nouveau royaume ; c'est alors que le *Domesday Book,* cette source incomparable de l'Angleterre du XIe siècle naquit en 1086.

1106. Il est considéré jusqu'à présent comme l'un des plus précieux trésors incontournable des Archives Nationales du Royaume-Uni. En 1986, le BBC a lancé un nouveau projet appelé *Domesday*[481] se fixant comme objectif de documenter à l'aide de l'informatique la vie ordinaire du Royaume-Uni à la fin du siècle passé. Toute la documentation était publiée sur des disques optiques de 12 pouces, une technologie très moderne en ce temps-là. Les organisateurs du projet avaient l'intention de répéter le projet tous les vingt-cinq ans pour illustrer les changements et préserver les données[482].

1107. En 1999, il s'est avéré que l'environnement informatique (matériel et logiciel) du projet du 1986 avait été complètement changé, n'existant quasiment plus; ainsi toute la documentation était devenue inaccessible. (alors que les documents de Guillaume restaient bien lisibles après plus de neuf cent treize ans.).

[481] *The Story of the Domesday Project* [En ligne : http://www.bbc.co.uk/history/domesday/story].
[482] KECSKEMETI (C.) et KORMENDY (L.), *Op. cit., p.*199 s.

1108. Pour remédier à cette catastrophe et sauver la base de données, un autre projet a été lancé en urgence la même année nommé CAMiLEON[483] et, grâce aux spécialistes britanniques et américains, ils ont réussi, après plusieurs années de travail, de ranimer (par émulation) la documentation. Le projet *Domesday* est devenu le symbole de l'obsolescence numérique.

1109. Au tournant de 2002 et 2003, les informaticiens de l'Office exécutif du président des Etats-Unis ont changé le matériel et le logiciel du bureau. Cela avait pour conséquence de faire disparaitre vingt-deux millions d'emails.

1110. Ainsi ces deux exemples illustrent le risque de l'obsolescence numérique dans le temps et que la conservation du support numérique est beaucoup plus complexe que celle du support papier ; L'environnement informatique est évolutif et de nombreux paramètres doivent être pris en compte : matériel informatique, logiciel, format de fichier afin de pouvoir lire le document électronique conservé plusieurs années après sa création.

1111. Nous apprenons des deux exemples cités dessus que les méthodes d'archivage doivent évoluer en même temps que le matériel informatique et les logiciels et de permettre la lecture des documents archivés quelle que soit la méthode de conservation utilisée à l'origine.

[483] *Migration: A Camileon Discussion Paper, ARIADNE Web Magazine for Information Professionals*, [En ligne: http://www.ariadne.ac.uk/issue29/camileon].

II. Méthodes de conservation pérenne des documents électronique basées sur le choix de l'application logiciel et le support informatique.

A. Choix du matériel informatique procurant un accès facile aux documents électroniques au fil du temps

1112. L'idée ici vient d'une proposition prononcée par un projet de recherche ambitieux intitulé '*Projet InterPARES*' sur la préservation à long terme de l'authenticité des documents d'archives numériques[484].

1113. Ce projet a pour objet principal d'élaborer des lignes directrices s'appliquant à divers types de publications, de documents et de données numériques, et particulièrement importants pour les documents d'archives numériques à maintenir pour un laps de temps assez long.

1114. Un 'document transférable électronique' a besoin d'un logiciel facile à utiliser et un format de lecture accessible. Il fallait choisir un bon matériel informatique, un logiciel approprié et un format de fichier qui semble être le plus prometteur pour assurer un accès facile au document électronique au fil du temps.

1115. La première chose à voir dans le processus d'archivage électronique est la mise à disposition d'un logiciel approprié et pérenne pour accéder aux documents électroniques. Idéalement le logiciel utilisé doit permettre de garder pour le document électronique la même apparence au fil du temps pour en préserver l'accessibilité et l'intelligibilité.

1116. Nous entendons par 'logiciel approprié' une application informatique étant en mesure d'assurer que tous nouveaux logiciels seront capables de lire les anciens documents dans le format du logiciel sous lequel nous avons gardé et de les afficher à l'écran dans leur forme documentaire initiale.

[484] Voir *Supra* n°907.

1117. Techniquement, il s'agit de veiller à la rétrocompatibilité des nouveaux logiciels. Citons un exemple illustratif assez fréquent sur le document électronique de format 'Word' ; lorsque nous installons sur le PC une version récente de Microsoft Office, comme par exemple MS Office 2016, puis nous utilisons cette version ouvrir un document que nous avions précédemment crée utilisant une version antérieure de MS Word (disons MS Word 2013), nous posons la question si le document s'affichera correctement en préservant le contenu et la même apparence et forme documentaire sur cette version plus récente de logiciel.

1118. Il est ainsi très important d'utiliser des logiciels compatibles avec les versions antérieures (la *rétrocompatibilité*[485]) ou les versions subséquentes (la *post-compatibilité*[486]), ce qui n'est pas évident dans la plupart des logiciels que nous utilisons ; ce qui rend par conséquent l'accès aux documents d'archives limité et difficile à long terme.

1119. Il est également important que les logiciels destinés à une seule application fonctionnent bien avec ceux des autres applications et systèmes. C'est la faculté d'opérer avec différents matériels et logiciels, ce qui réduit la dépendance des documents électroniques des produits informatiques[487]. Le terme scientifique exact pour décrire cette fonctionnalité est l'*interopérabilité*[488].

1120. D'ailleurs, les logiciels devraient pouvoir recevoir et fournir des fichiers dans un certain nombre de formats différents. Ainsi il nous sera plus facile d'accéder aux documents et également de les déplacer vers d'autres systèmes. Suivons l'exemple ci-dessus sur le MS Office, le logiciel MS Word nous donne

---

[485] La rétrocompatibilité est un terme informatique qui correspond à la capacité d'un appareil ou d'un programme à respecter les informations, consignes et périphériques préalablement enregistrés dans le système précédent. [En ligne : http://www.linternaute.com/dictionnaire/fr/definition/retrocompatibilite/].

[486] La post-compatibilité est un terme informatique qui désigne la compatibilité pour un programme informatique avec des versions ultérieures dans le sens où les informations enregistrées dans un logiciel pourraient être affichées et sauvegardées dans des versions subséquentes.

[487] Charles Kecskemeti et Lajos Kormendy, *Op., cit., p. 126.*

[488] L'interopérabilité ou interfonctionnement en informatique est la capacité que possède un système informatique à fonctionner avec d'autres produits ou systèmes informatiques, existants ou futurs, sans restriction d'accès ou de mise en œuvre. Les deux termes sont normalisés par la CSA et la Commission électrotechnique internationale (*ISO/IEC 2382-18:1999*). Aussi voir *Supra* n°729 sur la notion de l'interopérabilité.

une multitude d'options de formats que nous pourrons utiliser pour enregistrer le document crée (i.e. doc, docx, pdf, txt, xml).

B. Préservation des supports physiques des documents électronique

1121. Un bon archivage électronique ne peut pas négliger la conservation physique des supports qui portent les données. Il s'agit ici de deux catégories de supports utilisées pour le stockage de longue durée.

1122. La première catégorie comprend le support magnétique. Pour les documents électroniques, nous nous intéressons particulièrement au disque dur magnétique[489] qui représente le support sur lequel les documents électroniques peuvent être gardés.

1123. D'autre coté, il y a le support optique qui comprend deux types principaux, d'abord, un CD ("*Compact Disc*")[490] qui est un disque optique, inventé en 1978, utilisé pour stocker les données sous forme numérique.

1124. Etant un autre support semblable à celui de CD pour la sauvegarde et le stockage de données, le DVD[491] ("*Digital Versatile Disc*") est un disque optique numérique dont l'enregistrement se fait par rayon laser.

1125. Dans les années 80, la conservation de l'information numérique a été examinée par les organismes responsables de la préservation des informations produites par les institutions sous forme de traitements de textes tels que les archives. L'attention s'est ainsi portée sur la fragilité du support qui était alors essentiellement magnétique.

---

[489] Le disque dur magnétique est l'espace physique de stockage des données sur un ordinateur. [En ligne : http://www.dicodunet.com/definitions/materiel/disque-dur.htm].

[490] Le terme 'Disque Compact' désigne un disque numérique de 12 centimètres de diamètre à lecture par laser. (On dit aussi communément *disque compact* ou *compact* ou, par abréviation, CD.), [En ligne : http://www.larousse.fr/dictionnaires/francais/Compact_Disc_Compact_Discs/17591].

[491] Le *DVD* est défini comme « Format de disque optique numérique de grande capacité destiné à remplacer le *CD-ROM*, le *CD-I* et le *CD vidéo* ».
[En ligne : http://www.larousse.fr/dictionnaires/francais/DVD/27067?q=DVD#431176].

1126. Les disques optiques ont beaucoup d'avantages par rapport aux disques durs magnétiques; Ils sont plus stables, leur durée de vie est plus longue et utilisés à grande échelle.

1127. Les disques optiques sont faciles à manipuler et que les données enregistrées par voie de gravure laser ne sont pas altérables ; pourtant il faut éviter les disques réinscriptibles pour prémunir contre la perte ou toute modification de données. C'est que ces derniers permettent aux utilisateurs de remplacer les fichiers enregistrés sur le disque.

1128. D'ailleurs, la capacité du support optique est relativement limitée par rapport au support magnétique, mais elle croit rapidement.

1129. Concernant l'endurance et la longévité des CDs, selon les tests de vieillissement les CD enregistrables gravés se montrent plus fragiles que les CD pressés. Il n'y a malheureusement pas de norme établie pour mesurer la durée de vie probable d'un CD.

1130. Nous retenons de tests annoncés par des laboratoires, tel que le *National Media Lab*, que la durée de vie moyenne pour un CD enregistrable est plutôt de l'ordre de cinq (5) ans, et pour le CD pressé elle va de dix (10) à vingt-cinq (25) ans[492].

1131. Il est évident qu'il est plus favorable aujourd'hui d'utiliser les DVDs pour conserver les données informatiques. C'est que ces derniers permettent d'engranger une plus grande quantité de données sur un disque de même taille. La capacité standard pour un DVD est de 4,7 Go, et 8,5 (double couche).

1132. Par contre, nous reprochons au DVD le risque de la diminution de la durée de vie, en raison de la seule augmentation de densité des données.

[492] Catherine Lupovici, *Les stratégies de gestion et de conservation préventive des documents électroniques* - juillet 2000. [En ligne : http://bbf.enssib.fr/consulter/bbf-2000-04-0043-004].

1133. Les études de vieillissement « naturel » des premiers disques conservés dans de bonnes conditions montrent un vieillissement des vernis protecteurs de la couche métallique qui peut entraîner son oxydation[493].

1134. Pour cette raison, les affirmations des fabricants de certains supports, CD et DVD notamment, selon lesquelles leurs produits dureront cent ans, n'ont qu'une importance théorique. L'obsolescence du matériel et du logiciel sera certainement plus rapide. Il ne sert donc à rien d'avoir un support durable si le matériel et le logiciel compatible font défaut.

1135. Les supports aussi changent et se développent très rapidement, les normes tombent en désuète en dix à quinze ans, ce qui signifie que les supports que nous utilisons aujourd'hui ne seront probablement plus lisibles dans moins de vingt ans.

1136. Les supports optiques craignent particulièrement la flexion et la rayure. Il est recommandé de porter des gants doux quand nous manipulons les disques afin de les protéger des empreintes qui peuvent les rendre illisibles.

1137. Au nettoyage, il ne faut pas utiliser des solvants, la poussière ou la pollution légère doivent être éliminées par pinceau ou par textile. Il est très important que les lecteurs et les graveurs soient propres et entretenus. Il ne faut pas laisser les disques dans les lecteurs.

1138. Afin d'éviter les pertes d'information, les supports magnétiques ne doivent pas être stockés à proximité de câbles, de blocs d'alimentation ou d'autres appareils qui génèrent des champs magnétiques. Le volume de pertes éventuelles dépend de la force du champ, de la distance et de la durée de l'exposition, en sorte que même un effet faible peut être nocif s'il dure longtemps. Les disques doivent être stockés en position verticales[494].

[493] M. Vivant, *Op. cit.*
[494] *Ibid.*

1139. Il faut aussi éviter la température et l'humidité relativement élevées ainsi que leurs fluctuations, parce qu'elles peuvent fragiliser la matière du support, décoller la couche magnétique. Pour le stockage pérenne des supports magnétiques, la température recommandée est de 18+-1C et l'humidité relative doit être de 45+-5%.

1140. Les exigences climatiques pour le stockage des disques optiques sont pareilles à celles des supports magnétiques. La conservation à basse température ralentit le processus de vieillissement des supports. La fluctuation de l'humidité relative ainsi que de la chaleur accélèrent les processus nocifs. L'humidité relative au dessus de 60% facilite le développement des moisissures.

1141. Le soleil direct est dangereux pour les disques aussi. Il ne faut pas les stocker en tas parce qu'ils peuvent se déformer. Leurs boites plastiques d'origine les protègent de la déformation.

1142. Les opérations de conservation exigent matériel et logiciel. Si nous travaillons avec beaucoup de CD, nous avons besoin d'un outil approprié. Nous pouvons aussi acheter des logiciels spéciaux pour la surveillance et la conservation (*repository management software*)[495]. Ces logiciels identifient automatiquement des données, contrôlent leur intégrité, procèdent en temps voulu au rafraichissement et, conformément aux instructions, à la migration des fichiers.

1143. Il est fortement recommandé de conserver les documents électroniques en plusieurs exemplaires. Ainsi les archivistes ont mis en œuvre, au début des années 90, un rafraîchissement du support de l'information en recopiant périodiquement les données d'un support sur un autre. Cette technique reste efficace tant que l'information est encodée dans un format indépendant de la plate-forme matérielle et logicielle qui a servi à la produire et à l'utiliser, et tant que le logiciel qui sert à interpréter le format d'encodage est maintenu ou qu'il est remplacé par

[495] Actes de la Ve conférence du DLM-Forum « *La gestion de l'information et des archives électroniques en Europe : réalisations et nouvelles directions, Toulouse* », Direction des Archives de France, décembre 2008, p.64. [En ligne : http://www.archivesdefrance.culture.gouv.fr/static/2768]. Voir aussi : DELPIERRE (N.), HIRAUX (F.) ET MIRGUET (F.), *Les chantiers du numérique – Dématérialisation des archives et métiers de l'archiviste, Louvain-la-Neuve* 2012.

une nouvelle version qui assure la compatibilité ascendante avec au moins la version précédente.

III. Rafraichissement des supports et les systèmes de conversion

1144. Afin de maintenir les documents électroniques fonctionnels pour une longue durée, il convient de gérer le rafraîchissement des supports en disposant d'outil de gestion de l'espérance de vie de tous les supports de tous les documents.

1145. Pour ce faire, il faut respecter certains critères relevant de la forme et le contenu du document, puis d'envisager les différentes stratégies techniques utilisées pour le rafraichissement des supports.

1146. Veiller à ce que le contenu et la forme des documents numériques maintenus en tant que documents d'archives soient stables et fixes[496]. Un des grands avantages des documents numériques est la facilité avec laquelle il est possible d'éditer, de réviser ou de mettre à jour l'information. Pourtant, cela signifie également que l'information essentielle peut être modifiée ou même perdue, accidentellement ou volontairement. Il s'agit d'un problème particulièrement important pour les documents d'archives, puisqu'une des caractéristiques d'un document d'archives est que son contenu doit être inchangé et inchangeable.

1147. Autrement dit, l'information et les données d'un document d'archives ne devraient pas être écrasées, modifiées, supprimées ou étoffées. Un système qui contient un flux d'information ou de données en constante évolution ne comprend pas réellement des documents d'archives tant que quelqu'un ne décidera pas de les créer et de les enregistrer sous une forme fixe et avec du contenu stable.

[496] Il s'agit de l'une de recommandations du Projet InterPARES 2 pour la préservation à long terme de l'authenticité des documents d'archives numériques. [En ligne : http://www.interpares.org/].

1148. Bien que la notion de contenu stable soit plutôt simple, celle de la forme fixe est plus complexe. Essentiellement, il signifie que le message communiqué par un document d'archives numérique (ou un autre objet numérique) peut s'afficher à l'écran dans la même présentation documentaire que celle qu'il avait lors de son élaboration ou de sa réception et de son enregistrement initial.

1149. Les trains de bits qui composent le document d'archives numérique et déterminent sa présentation numérique (c.-à-d. son format de fichier) peuvent changer, mais sa présentation documentaire doit demeurer inchangée. Par exemple, lorsqu'un document créé dans un format Microsoft Word puis enregistré dans le format Adobe PDF, la présentation numérique du document est modifiée – en passant du format de fichier .doc de Microsoft Word au format de fichier .pdf d'Adobe – mais sa présentation documentaire, également appelée forme documentaire, ne change pas. En conséquence, il est possible d'affirmer que le document a une forme fixe.

1150. La question de la présentation documentaire des documents numériques est particulièrement importante au maintien et à l'évaluation de la fiabilité et de l'exactitude des documents d'archives. Toute mise à niveau, conversion ou migration ultérieure des données peut entraîner une modification de la forme documentaire.

1151. Il serait donc judicieux de présenter les différentes stratégies techniques ayant pour objectif de garantir la pérennité de l'encodage du document électronique qui se trouve dresser sur un support électronique[497].

A. La technique de Migration

1. Contexte et notion.

1152. L'évolution des supports et des langages machine ne devraient pas conduire à négliger l'enquête sur la préservation de l'écrit électronique dans le temps. La pérennité du 'document transférable électronique' peut être garantie

[497] JOLY-PASSANT (E.), *Op. cit., p.*482 s.

par le bais d'opérations d'archivage et de "migrations" régulières sur des supports appropriés.

1153. La technique de Migration est définie comme une *méthode de transfert périodique d'une ressource électronique d'un environnement matériel/logiciel à un autre, ou d'une génération de technologie informatique à une autre*[498].

1154. De cette définition, nous retenons que la migration s'effectue sur un document électronique qui relève d'une ancienne génération technologique pour le rendre opérable à nouveau sans avoir de souci par rapport à son accessibilité, son intégrité et la gestion de données. Techniquement parlons, la migration porte essentiellement sur la modification de format des objets numériques tout en préservant leur contenu inchangé.

1155. Ainsi la migration doit préserver l'intégrité de l'objet numérique, tout en permettant à l'utilisateur de continuer à l'utiliser. Cela implique que l'utilisateur saura par exemple dans la nouvelle version effectuer des recherches d'information et d'afficher les données de manière identique que dans la version originaire.

1156. Cette technique de migration est mise en œuvre chaque fois que la technologie change. Alors nous effectuons les changements d'environnement informatique nécessaires pour rendre le document re-accessible. Puisque les formats changent, il faut opérer la migration de temps en temps.

1157. La preuve de succès de la technique de migration est témoignée par le fait que la plupart des services d'archives qui pratiquent l'archivage électronique ont choisi la technique de migration sur l'ensemble de leurs données numériques.

1158. Il convient aussi de rappeler que le législateur français a reconnu la preuve par écrit indépendamment du support et des modalités de transmission utilisés et respecte ainsi le principe de neutralité technologique. Il s'agit d'une acceptation

[498] Catherine Lupovici, *Les stratégies de gestion et de conservation préventive des documents électroniques*, Bibliothèque Nationale de France, *BBF 2000* - Paris, t. 45, n° 4.

tacite de la loi pour admettre la mise en en œuvre de la technique de migration afin de maintenir les documents juridiques dans le temps.

2. Les défis relevant de l'opération de migration

1159. Comme toute chose dénuée de perfection, aussi la technique de migration a ses failles. S'il est bien clair que la migration signifie que le document électronique soit converti de formats obsolètes en formats conformes aux normes nouvelles ; lors du choix des nouveaux formats, nous tenons compte de la qualité et de la durabilité de l'opération effectuée sur le document.

1160. Au cours de la migration, la perte de données est probable. Nous devons veiller à réduire au minimum les pertes de contenu, de métadonnées[499] et de données qui représentent des fonctions importantes ; aussi en ce qui concerne les fautes d'affichage de la forme du document.

1161. D'avantage, les migrations consécutives des documents électroniques dans le sens où nous nous mettons à convertir encore et encore les documents déjà migrés, résulte éventuellement l'accumulation des pertes.

1162. Cela signifie que chaque fois que nous effectuons une migration sur des données pré-migrées, cette répétition menace la sécurité des documents ; c'est la raison pour laquelle il est fortement conseillé d'y procéder le plus rarement possible, en intercalant de longs intervalles.

1163. Il est aussi recommandé de vérifier de temps en temps les documents déjà migrés et, comme dans le long terme l'environnement informatique change, de nouvelles migrations seront inévitables. Elles devront intervenir par périodes

[499] D'après une définition courante, les métadonnées sont des données sur des données (documents). Dans le monde numérique, leur rôle s'est considérablement accru parce que dans la plupart des cas, les éléments constitutifs du document apparaissent comme des métadonnées : on se réfère au support par m métadonnées techniques, l'identifiant est une métadonnée et naturellement on décrit par métadonnées la structure et le contexte. Elles sont accolées aux documents natifs comme aux images scannées. Les métadonnées techniques étant indispensable à l'entretien et à la migration, il faut ainsi surveiller quels sont et ou se trouvent les fichiers ayant des formats menacés d'obsolescence. Voir JOLY-PASSANT (E.), *Op. cit.*, p.123 s.

déterminées, par exemple tous les dix ans, ou avant le changement du système d'exploitation.

1164. Pour encore mieux assurer le bon fonctionnement de l'opération de migration, il est conseillé de faire la conversion sur les fichiers originels ; et pour détecter les pertes, le logiciel qui fait la conversion doit signaler automatiquement les documents ayant été touchés dans leur intégrité[500].

1165. Il convient aussi de signaler que le choix du format est essentiel, car si nous utilisons des formats durables, la nécessité de migration arrivera plus rarement.

B. Méthode de l'émulation

1166. Dans les domaines de l'informatique, le terme émulation est employé au sens de simulation et d'imitation l'acception du mot est influencé par les termes anglais '*emulation*' et '*emulator*'.

1167. Ce terme décrit un principe général consistant à remplacer un système par un autre sans changement du fonctionnement d'un point de vue externe. En d'autres termes, l'émulation signifie que nous imitons l'environnement informatique originel, le matériel et le logiciel, par des logiciels spéciaux qui s'appellent '*émulateurs*'. L'émulation rend possible l'utilisation des documents électroniques par leur logiciel originel malgré le nouvel environnement informatique.

1168. L'un des atouts majeurs de l'émulation consiste à pouvoir préserver le document dans son format original, ce qui ne compromet ni sa forme ni ses fonctionnalités, ni même son « *look and feel* »[501].

---

[500] Voir aussi http://www.nationalarchives.gov.uk/aboutapps/pronom/#documentation, ainsi que David HOLDSWORTH, *Installment on "Preservation Strategies on Digital Libraries" (DCC Digital Curation Manual 2007*) p. 12-13. Plusieurs services d'archives possèdent parallèlement : *1. Les fichiers originels 2. Les fichiers de préservation ; 3. Les fichiers de communication. La conservation des fichiers originels sert à la sécurité parce que si la conversion rate, on peut répéter l'opération. C'est la politique des Archives nationales du Royaume Uni et le projet CEDAR recommande la même méthode*.

[501] F.Boudrez, *The digital recordkeeping system : inventory, information layers, and decision-making model as point departure, in Project DAVID*, http://www.law.kuleuven.ac.be.icri, p. 12.

1169. L’émulation consiste à émuler un environnement informatique différent de la plate-forme sur laquelle se fait l’émulation. Par exemple, nous pouvons imaginer d’émuler un Macintosh d’une certaine version sur un PC avec Windows NT, de manière à pouvoir utiliser un cédérom initialement publié pour Macintosh seulement.

1170. C’est comme si nous voulons maintenir un poisson en vie en lui faisant sortir de l’eau. Pour garder le poisson en vie, il faut le mettre dans un aquarium de taille décente, rempli d’eau afin de lui procurer un environnement semblable au sien pour pouvoir survivre le monde externe.

1171. Un émulateur pour les vieux documents électroniques a la même fonction qu’un aquarium pour les poissons. Afin de garder les documents en plein fonctionnalité, nous nous servons de la méthode d’émulation pour leur préserver l’ancien environnement et le matériel nécessaire pour leur survie.

1172. Un émulateur est un outil qui fait arrêter le temps à un document électronique et son accompagnement ; et nous entendons par accompagnement le logiciel qui sert à le faire fonctionner.

1173. Alors au lieu de faire évoluer les documents électroniques, en procédant à leur migration pour modifier leur format et les convertir pour suivre la nouvelle technologie et les rendre opérationnels, nous les préservons dans leur environnement informatique originel afin qu’ils restent accessibles sous leur ancien environnement imité.

1174. Le recours à un émulateur, selon le contexte, permet de faciliter le développement ou le débogage d'un système ou de remplacer un système obsolète ou inutilisable par un autre. Dans ce cadre, il est possible de faire fonctionner le nouveau système, l'émulateur, de la même manière que le système imité[502].

[502] Il faut distinguer entre l’émulation et la simulation. Il faut voir dans l'émulation une imitation du comportement physique d'un matériel par un logiciel, et ne pas la confondre avec la simulation, laquelle vise à imiter un modèle abstrait. L'émulateur reproduit le comportement d'un modèle dont toutes les variables sont connues, alors que le simulateur tente de reproduire un modèle mais en devant extrapoler une partie des variables qui lui sont inconnues (exemple : la simulation du comportement d'un trou noir).

1175. La technique de l'émulation appliquée à la préservation à long terme des ressources électroniques signifie que nous cherchons à définir une méthode qui va permettre d'émuler des systèmes informatiques obsolètes sur les systèmes encore inconnus du futur.

1176. La mise en œuvre de l'émulation implique les trois critères suivants[503] :

- le développement de techniques généralisables pour la spécification d'émulateurs qui tourneront sur des ordinateurs futurs et qui permettront d'enregistrer tous les attributs nécessaires à la recréation du comportement des documents actuels et futurs ;
- le développement de techniques pour enregistrer les métadonnées nécessaires pour chercher, accéder aux documents numériques et les recréer;
- le développement de techniques pour encapsuler les documents, leurs métadonnées, les logiciels et les spécifications des émulateurs de façon à prévenir leur altération.

1177. Egalement, l'émulation nécessite une expertise par informaticiens qualifiés, parce qu'il faut faire fonctionner non seulement le système d'exploitation et le logiciel d'application, mais aussi tous les fichiers nécessaires pour le fonctionnement de ce dernier. En plus, il faut décrire les spécifications d'émulateur, c'est-à-dire tous les attributs (par exemple vitesse, attribut d'affichage, outils et périphériques) du matériel originel qui rendront possible la reprogrammation future de l'émulateur actuel[504].

1178. Selon ses partisans dont la plupart sont des informaticiens, en ayant recours à l'émulation nous pouvons éliminer les inconvénients de la migration, par exemple le changement de la forme des documents, la détérioration de l'authenticité et de l'utilisabilité, et les pertes accumulées qui résultent des conversions consécutives dans le long terme.

---

[503] Catherine Lupovici, *Les stratégies de gestion et de conservation préventive des documents électroniques, BBF* 2000 *Paris*, t.45, n.4. p.4

[504] Jeff Rothenberg donne un bon résumé sur l'émulation (bien qu'il manqué d'objectivité) dans '*Avoiding Technological Qicksand: Finding a Viable Foundation for Digital Preservation*' (*Council on Library and Information Resources, Washington 1999*).

1179. Tout cela est vrai, et pourtant les centres d'archives hésitent toujours à appliquer l'émulation. Ils estiment que le système d'émulation présente aussi certains inconvénients qui ne peuvent pas passer inaperçus. Les inconvénients éventuels de l'émulation sont les suivants :

- Apprendre à utiliser les logiciels d'application originels dont le nombre augmente sans cesse peut causer de grandes difficultés aussi bien aux archivistes qu'aux chercheurs.
- En quelques décennies, un service d'archives peut accumuler plusieurs centaines de logiciels.
- A cause du changement continu de l'environnement du matériel et du logiciel, il faut produire de plus en plus d'émulateurs qui a leur tour doivent être renouvelés encore et encore à la suite des changements intervenus.
- Les logiciels propriétaires impliquent souvent une redevance de licence qui peut couter très cher en cas d'accumulation
- Les nombreux agrégats de données distincts, traités par autant de logiciels rendent difficile de développer un système de recherche unifié et compliquent l'accès aux données par l'Internet.

1180. Malgré ces arguments, il ne faut pas exclure l'émulation de la vie de centre d'archivage, parce que certains documents électroniques peuvent avoir des fonctions importantes qui ne peuvent être conservées par migration mais seulement par émulation.

1181. D'ailleurs, les inconvénients cités dessus ne sont pas bien graves et ne touchent pas à l'utilisabilité et l'intégrité des documents faisant l'objet de l'émulation. D'après le professeur canadien David Bearman, '*sont à conserver les dossiers et pas les fonctions du système informatique ; il ne faut pas confondre dossier et information*[505]'. Cette phrase illustre les craintes évoquées par les archivistes que sauvegarder l'utilisabilité ne signifie pas un avantage en soi, parce que dans les systèmes de gestion des documents des producteurs, il y a des fonctions (par exemple enregistrer, modifier et effacer des données, interrogations

[505] Cité par Stewart GRANGER, "*Emulation as a Digital Preservation Strategy" in D-Lib Magazine*, Octobre 2000, vol.6. No. 10. [En ligne : http://www.dlib.org/dlib/october00/granger/10granger.html].

relatives à certaines procédures) qui sont inutiles, voire indésirables pour les archives.

1182. Il y a aussi des projets d'émulation qui ont connu beaucoup de réussite, nous citons par exemple le *Global Access to Emulation Services (GRATE)* développé par l'Université de Fribourg-en-Brisgau en Allemagne dans le cadre du projet européen *PLANETS*, l'émulateur *Dioscuri*[506], développé sous la direction des spécialistes hollandais pour PC de x86 ou encore les résultats et les outils du projet *KEEP (Keeping Emulation Environment Portable)* financé par l'Union européenne.

1183. Pour conclure, les deux dispositifs technologiques de 'migration' et 'émulation' réalisent leur objectif de rafraîchissement des supports électroniques, bien que chacun dispose d'un mécanisme particulier pour y parvenir. Dans la société de l'information, les consultants techniques font plus de recours à la migration que l'émulation pour les besoin de leur entreprises, préserver les données et s'adapter aux changements d'environnement informatique. Ainsi nous estimons que la migration est une méthode de transfert plus appropriée aux 'documents transférables électroniques'.

[506] [En ligne : http://www.planets-project.eu/, http://www.planets-project.eu/docs/reports/Planets_PA5-D7_GRATE.pdf].

CONCLUSION DU CHAPITRE II

1184. La possession est une notion du droit des biens, un aspect estimé inhérent au document papier, dont l'équivalent électronique ne pourrait pas se prévaloir. Cependant, La dématérialisation de la possession en application de la théorie *corpore alieno* permet au possesseur de se séparer matériellement de son bien au profit d'un autre ; ce détachement de la chose ouvre la voie vers l'utilisation du 'document transférable électronique' en tant que possession *corpore alieno*.

1185. Afin de transposer la notion de la possession dans un environnement électronique, nous étions à la recherche d'un critère fonctionnel souple. C'est le critère du contrôle qui est exemplaire. Il implique que la personne exerçant le contrôle du 'document transférable électronique' est jugée « porteur habilité » à s'en prévaloir.

1186. Pour identifier le « porteur habilité », il y a deux modèles principaux :

- Le modèle du support, selon lequel l'identité de la personne 'porteur' figure dans le document électronique proprement dit, et tout changement de propriété se trouve automatiquement consigné dans le document électronique. Cette technique de sécurité intrinsèque au document est protégée par un mot de passe ou bien une autorisation biométrique.
- Le modèle du registre, selon lequel l'identité du porteur est consignée dans un registre géré par un prestataire de services de confiance en tant que garant de la sécurité.

1187. Nous privilégions le modèle du registre pour les 'documents transférables électroniques', car ce modèle fait intervenir des prestataires de service de confiance qualifiés qui garantissent la sécurité du document, la certification et l'horodatage électronique.

1188. Suite à l'exécution du 'document transférable électronique', nous avons recours au système d'archivage pour sauvegarder le document dans un environnement informatique. Cette conservation pérenne du document électronique est assurée par un logiciel 'retro-compatible', un support physique (CD, DVD) et des systèmes de conversion appropriés pour préserver l'intégrité du document électronique dans le temps (i.e. Migration et émulation).

CONCLUSION

DE LA DEUXIÈME PARTIE

1189. Dans un environnement informatique, l'exécution du 'document transférable électronique' n'obéit pas aux mêmes règles que celles du document papier. Il est plus adapté de lui appliquer des règles équivalentes pour assurer son exécution.

1190. D'une part, la notion de l'unicité qui caractérise le document papier est traitée dans l'environnement informatique sous l'angle de l'unicité technique ; un document électronique doit d'abord satisfaire à l'exigence de l'originalité décrite comme nous l'avons vu à l'article 8 de la Loi type de la CNUDCI. L'unicité technique est soutenue par le recours à un exemplaire faisant foi.

1191. D'autre part, le document électronique n'a pas de support matériel permettant d'appliquer les exigences de la possession et de ses éléments constitutifs de la possession (*corpus* et *animus*) qui existent dans les documents papier. Cependant, la possession *corpore alieno* permet le détachement de la chose possédée de son possesseur. Pour les 'documents transférables électroniques', celle-ci se traduit par un nouveau critère, celui de 'contrôle', équivalent fonctionnel de la possession dans un 'document transférable électronique', qui signifie que la personne qui exerce le contrôle du 'document transférable électronique' est jugée porteur habilité à s'en prévaloir.

1192. La personne qui détient le contrôle sur le 'document transférable électronique' peut être identifiée par le biais du modèle du registre géré par un prestataire de services de confiance qualifié, qui prend en charge les services de certification et d'horodatage électronique pour garantir la sécurité du document.

CONCLUSION GÉNÉRALE

1193. L'évolution de l'internet et les NTIC (nouvelles technologies de l'information et de la communication) ont irrémédiablement changé le comportement des gens ; toute personne a aujourd'hui le réflexe d'agir via l'internet plutôt que de créer un document manuscrit et d'utiliser la poste pour envoyer ce document à son destinataire. C'est aussi le cas pour les instruments financiers. Ce travail fut consacré à l'examen de l'environnement informatique propre à sécuriser les échanges et la circulation des instruments financiers.

1194. Concernant la protection de la vie privée, nous pouvons songer aux dangers résultant des traitements automatisés des données personnelles, auxquels les moyens de communication électroniques viennent donner une dimension nouvelle. L'impératif de protection de la vie privée est difficile à satisfaire au regard des possibilités infinies qu'offre l'informatique.

1195. Pour concilier le droit au respect de la vie privée avec la liberté de circulation des données, il y avait la transposition en droit français de la Directive européenne 95/46/CE du 24 octobre 1995 par la loi du 6 août 2004 ayant modifié la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; celle-ci va évoluer en raison du Règlement européen 2016/679 du 27 avril 2016[507].

1196. Ce règlement du 27 avril 2016, faisant suite à la directive du 24 octobre 1995, vise à la généralisation de l'outil informatique dans le quotidien en accordant une protection renforcée aux données à caractère personnel.

1197. L'apparition du phénomène '*Big data*' et du *Cloud*, a placé la barre très haute pour le législateur européen en termes de protection des données personnelles. Le *Big data* s'appuie sur la collecte d'informations relevant forcément de la vie privée des personnes aux fins d'obtenir des résultats

[507] Romain Perray, *Fasc. 274-10 : Informatique - Données à caractère personnel - Introduction générale et champ d'application de la loi "Informatique et libertés*, 18 Mai 2016, date de la dernière mise à jour : 19 Octobre 2016, *JurisClasseur Administratif, LexisNexis*, n°19 et 20.

informationnels qui peuvent être exploités au bénéfice des entreprises et des établissements financiers. Ces différents risques d'atteintes à la vie privée se sont considérablement accrus avec le développement de ces techniques. Ils augmentent même d'un cran à chaque avancée technologique. À tel point que la réglementation a dû s'adapter elle aussi par phases[508].

1198. Un autre défi technologique est marqué par l'augmentation des demandes d'utilisation des services *Cloud computing*. Il est clair que l'Union européenne s'intéresse depuis quelques années au *Cloud computing* ou "informatique en nuage", dont les contours restent encore insaisissables[509]. S'agissant d'un mode d'externalisation de données dématérialisées par le biais d'Internet, le *cloud computing* prend des formes variées selon les offres proposées par les opérateurs (hébergement, fourniture de plateforme, logiciel en ligne,...). Il s'agit dés lors d'appréhender sinon de canaliser l'activité des opérateurs du Cloud. C'est assez difficile car il s'agit d'intervenants privés, qui agissent dans le cadre d'une activité privée et contractuelle.

1199. Un premier constat, les institutions financières ont recours aux services *Cloud computing* pour la gestion des "documents transférables électroniques", ce qui peut entraîner divers problèmes comme ceux relatifs, à la détermination des qualifications des prestataires de service *Cloud*, à la protection des données personnelles et à la localisation des données lorsque les serveurs sont à l'étranger. Il n'existe pas de législations qui viseraient à réglementer le *cloud*. Chaque prestataire offre des services particuliers aux entreprises, et l'accès au *cloud* est purement contractuel sans qu'il y ait d'uniformité dans les contrats de gestion de données ; ce qui pose problème aux entreprises c'est la localisation des *Datacenter* où sont conservés leurs données, la surveillance électronique des données par les État a focalisé à juste titre l'attention des entreprises sur la sécurisation de l'accès à leurs informations.

---

[508] V. sur l'importance de ces données dans le cadre de leur réexploitation par le *Big Data,* M. Lanna, *Le quantified-self, nouveau moteur du big data et menace pour la vie privée : LPA 12 mai 2016, n° 95, p. 6*

[509] B. Fauvarque-Cosson et C. Zolynski, *Le cloud computing, L'informatique en nuage : SLC 2014.* - E. Sordet et R. Milchior, *La définition des contours juridiques du cloud computing : Comm. com. électr. 2012, étude 18 ; Le cloud computing, un objet juridique non identifié : Comm. com. électr. 2011, étude 20 ; Dossier spécial "Contrats et cloud computing" : RLDI 2013, n° 98.*

1200. Un deuxième constat: dans le domaine juridique, les contrats électroniques aussi bien que les instruments financiers électroniques ne constituent pas une nouvelle catégorie de contrats ou d'instruments financiers. Ce sont des actes classiques comme les contrats de vente, service, mandat ou bien des chèques, des lettres de change ou des billets à ordre passés par voie électronique. Ils peuvent être soit exécutés en ligne soit en dehors du réseau. Mais à la différence des contrats ou instruments financiers manuscrits, les documents informatiques tiennent leur spécificité, de la technicité de la matière et de l'influence du droit d'auteur protégeant les logiciels ; d'autre part leur originalité se manifeste surtout lors de leur formation et de l'immatérialité du moyen par lequel ils sont conclus et exécutés.

1201. Il existe un lien indéniable existe entre la confiance et la sécurité technique. La confiance en matière de transactions électroniques s'entend du respect des exigences de sécurité technique sur lesquelles s'appuie la sécurité juridique.

1202. Aujourd'hui le 'document transférable électronique' bénéficie, au même titre que l'écrit sous forme papier, de la reconnaissance juridique nécessaire. Cette reconnaissance juridique est l'aboutissement d'efforts considérables pour sécuriser les transactions électroniques et atteindre la confiance longuement recherchée.

1203. Sur le plan technique, la sécurité est assurée par le développement de la signature électronique, les mécanismes cryptographiques de chiffrement et les services de confiance et l'horodatage électronique.

1204. Sur le plan organisationnel, les documents électroniques sont confiés aux prestataires qualifiés de services de confiance dont la mission est d'assurer l'intégrité de toutes données électroniques à leur disposition et garantir l'unicité du 'document transférable électronique'.

1205. Du point de vue juridique, au fil des années 2000, La CNUDCI a entamé de nombreux débats dédiés à l'étude des aspects juridiques du commerce électronique et à l'étude des 'documents transférables électroniques' ; les groupes

de travail au sein de la commission ont visé l'élaboration des règles modernes, équitables et harmonisées régissant les 'documents transférables électroniques' et le commerce électronique en général ; car les lois nationales qui transposaient la directive 1999/93/CE dans les législations des différents Etats membres étaient diverses et variées au sein du marché unique, et les exigences techniques différaient d'un pays à l'autre et d'un service à l'autre, et cette absence d'uniformisation nuisait à l'instauration de la confiance dans l'économie numérique[510].

1206. La CNUDCI était consciente de l'importance d'accroître la sécurité juridique, en coordonnant les mesures nationales de contrôle et en assurant la reconnaissance et l'acceptation mutuelles de l'identification électronique. Ainsi le Règlement européen 2016/679 du 27 avril 2016[511] a pour mission d'atteindre ces objectifs. Ce règlement, une fois approuvé et entré en vigueur, viendra s'imposer en lieu et place des différentes dispositions existantes, spécialement en matière de signature électronique mais aussi en matière d'horodatage, de lettre recommandée électronique, et d'autres services électroniques de confiance apparus tout au long de la décennie et qui ne pouvaient être pris en compte en 1999, comme l'identification et l'authentification électronique. Cette nouvelle législation européenne atteints un niveau plus élevé d'efficacité juridique, et contribue au processus d'harmonisation des différentes législations nationales, ce qui garantira une confiance plus large dans le commerce électronique, et particulièrement dans l'utilisation du 'document transférable électronique'.

1207. Les 'documents transférables électroniques' jouissent donc enfin d'un système juridique plus cohérent et harmonieux comme nous avons tenté de le démontrer dans cette thèse. Les mesures techniques et organisationnelles mises en

[510] Résumé de l'analyse d'impact accompagnant la proposition de règlement du parlement européen et du conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, p. 8.

[511] « *L'adoption d'une directive ne permettrait pas de résoudre les problèmes actuels d'interopérabilité dans le domaine des signature électronique, dus à des divergences dans la transposition de la directive 1999/93/CE. En revanche, un règlement qui est directement applicable sans interprétation, garantit une meilleure harmonisation et est par conséquent approprié pour atteindre les objectifs de la législation proposée* ». Voir aussi *supra* n°138 s.

œuvre permettent de garantir la sécurité et la confidentialité des données traitées pour le compte des usagers.

1208. Comme le disait Jean Giraudoux : « *Nous savons tous ici que le droit est la plus puissante des écoles de l'imagination. Jamais poète n'a interprété la nature aussi librement qu'un juriste la réalité* ». L'évolution des techniques contraint effectivement le juriste à faire preuve d'imagination et de souplesse pour s'adapter aux changements dans la société de l'information.

BIBLIOGRAPHIES

I. OUVRAGES GÉNÉRAUX

BONHOMME (R.)

- *Instruments de Crédit et de Paiement,* 10e éd. L.G.D.J – 2013

CHAPUT (Y.) et SCHODERMEIER (M.D.)

- *Effets de commerce, chèques et instruments de paiement :* PUF, *Coll. Droit fondamental, 2e éd. 1998.*

FERAL SCHUHL (Ch.) :

- *Cyber droit : le droit a l'épreuve de l'internet*, Dalloz, 6ème éd., 2010.

GAUTIER (p.-v) :

- *Propriété littéraire et artistique, PUF*, 7e éd., 2010.

GAVALDA (Ch.) - STOUFFLET (J.)

- *Instrument de paiement et de crédit, LexisNexis Litec,* 8ème éd., 2012.

GUEVEL (D.)

- *L'atomisation du droit cambiaire, Mélanges P, Simler, Dalloz,* 2006, p. 457 et s

HILAIRE (J.)

- *Introduction historique au droit commercial : PUF, Coll. Droit fondamental, 1986*

JEANTIN (M.) et LE CANNU (P.)

- *Instruments de paiement et de crédita – Entreprises en difficulté,* Dalloz, 6ème éd., 2003.

JACQUET (J.M.), DELEBECQUE (P.), CORNELOUP (S.) :

- *Droit du Commerce International, Dalloz,* 2ème éd., 2010.

LE CANNU (P.), GRANIER (T.), ROUTIER (R.)

- *Instruments de paiement et de crédit Titrisation, Dalloz,* 8ème éd., 2010. p.301.

PIEDELIEVRE (S.)

- *Instruments de Crédit et de Paiement***,** 5e éd. Dalloz – 2007.

PEROCHON (F.) et BONHOMME (R.)

- *Entreprises en difficulté, Instruments de crédit et de paiement : LGDJ,* 4e éd. 1999, n° 603.

KARL VON SAVIGNY (F.)

- « Traité de la Possession en Droit romain », traduit de l'allemand par CH. Faivre D'Audelange, *Imprimerie De Cosse et Gaultier-Laguionie*. 6e éd., 1841.

RIPERT (G.) et ROBLOT (R.)

- *Traité de droit commercial : LGDJ, 16e éd. 2000, t. 2, par Delebecque et Germain, n° 1912.*

SCHULTZ (Th.)

- *Réguler le commerce électronique par la résolution des litiges en ligne : une approche critique,* LGDJ, Bruylant, 2005.

STOUFFLET (J.)

- *Instrument de paiement et de crédit, LexisNexis - Litec,* 8ème éd., 2012.

SZRAMKIEWICZ (R.) et DESCAMPS (O.)

- *Histoire du droit des affaires, 2e édition, LGDJ, (22 octobre 2013)*

THIEFFRY (P.)

- *Commerce électronique : droit international et européen, Litec*, 2002.

TERRE (F.), SIMILER (Ph.) et LEQUETTE (Y.) :

- *Droit civil, les obligations, Dalloz,* 9ème éd., 2007.

VIVANT (M.) et al. :

- *Lamy droit de l'informatique et des réseaux, Lamy*, 2011.

II. OUVRAGES SPÉCIAUX ET MONOGRAPHIES ET THÈSES

A. OUVRAGES SPÉCIAUX

CAPRIOLI (E.):

- *Signature électronique et dématérialisation – Droit et Pratiques*, LexisNexis SA, 2015.

- *Droit international de l'économie numérique : les problèmes juridiques liés à l'internationalisation de l'économie numérique*, Litec 2ème éd., 2007.

DELPIERRE (N.), HIRAUX (F.) ET MIRGUET (F.)

- *Les chantiers du numérique – Dématérialisation des archives et métiers de l'archiviste*, Louvain-la-Neuve 2012.

JOLY-PASSANT (E.)

- *L'écrit confronté aux nouvelles technologies*, L.G.D.J, 2006.

MALLET-POUJOL (N.)

- *Traçage électronique et libertés, Paris : la Documentation française, DL* 2006, 120 pages.

PIETTE –COUDOL (Th.) :

- *Echanges électroniques, Certification et Sécurité*, Litec, 2000.

KECSKEMETI (C.) et KORMENDY (L.)

- *Les écrits s'envolent – la problématique de la conservation des archives papier et numériques*, Edition Favre SA, 2014.

ROLAND (H.) et BOYER (L.)

- *Adages du droit français : Litec, 4e éd.* 1999

STUBBS (E.)

- *Big Data Big Innovation – Enabling Competitive Differentiation through Business Analytics, edition John Wiley & Sons*, 2014, p.206.

Vladimir O. SAFONOV

- *Trustworthy* Cloud Computing, *Edition John Wiley and Sons*, Février 2016.

B. THÈSES

BAYALOVITCH (L.) :

- *Le droit international du change :* thèse, Lyon, 1935 - *Arminjon et Carry.*

BOURGEOS (C.) :

- *L'anonymat et les technologies de l'information*, thèse Paris V, 2003.

CACHARD (O) :

- *La régulation internationale du marché électronique,* LGDJ, Bibl. dr. Pr., 2002, préf. Ph. FOUCHARD.

DAURIAIS (I.) :

- *La signature,* Paris II, 1997.

GAUTRAIS (V.) :

- *Le contrat électronique international – Encadrement juridique,* Bruxelles, Bruylant, 2ème éd., 2002.

GRAHAM J.-A :

- *Les aspects internationaux des contrats conclus et exécutés dans l'espace virtuel*, Paris I, 2001.

LABARTHE (F.)

- *La notion de document contractuel,* LGDJ, Bibl. dr. Pr., 1994, préf. J. GHESTIN.

III. ARTICLES ET CHRONIQUES

ABALEA (Th.) :

- « La signature électronique en France, état des lieux et perspectives », *Recueil Dalloz* 2001 p.2835, Éd. 2011.

de LA PRESLE (A.) :

- « L'administration et l'*Echange de Données Informatisé (EDI)* », *AJDA* 1992 p.707, Éditions Dalloz.
- « l'Etat et la reconnaissance juridique des transactions effectuées par échanges de données informatisées. Du document électronique à la dématérialisation », *RFDA* 1992 p.700-708, Éd. Dalloz 2011.

ANTOINE (M.) GOBERT (D.) et SALAUN (A.) :

- « Le développement du commerce électronique : les nouveaux mérites de la confiance », in *Droit des technologies de l'information, regards prospectifs*, Cahiers du centre de recherche informatique et droit, n◦16, *Bruxelles, Brulant,* 1999, p.3 à 32.

ASSAYA (L.) et BAUCOUIN (V.) :

- « La signature électronique par cryptographie à clé publique », *JCP* éd. E, 2003, n◦4, 146, p.164.

AUTIN (J.L.) et IDOUX (P.)

- « Fasc. 4600 : Droit National des Communications électroniques », *JCP*, 15 Janvier 2011, mise à jour : 6 Février 2015.

AUVRET (P.)

- « Fasc. 4860: Application de la loi de 1881 à la communication en ligne », *Publicité des délits de presse*, 15 Mars 2006.

BARESCH (D.) et SION (C.) :

- « La directive européenne sur les signatures électroniques », *Les Petites Affiches*, 21 fév. 2002, n◦38, p.24.

BATELOT (B.)

- « Définition : *Big Data* », 1er septembre 2016, [En ligne : http://www.definitions-marketing.com/definition/big-data/].

BENSAMOUN (A.) et ZOLYNSKI (C.)

- « *Big data et privacy* : comment concilier nouveaux modèles d'affaires et droits des utilisateurs », *LPA* 18 août 2014, n° 164, p. 8.

BERNERS-LEE (Tim)

- *Weaving the Web*, *HarperSanFrancisco*, 1999 (ISBN 978-0-06-251587-2)
- "What is web 2.0", 30 septembre 2005. http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.

BISMUTH (Y.)

- « Droit de l'Informatique – Eléments de Droit A L'Usage des Informaticiens », éd. *L'Harmattan*, 2011.

BITAN (H.) :

- « La signature électronique : comment la technique répond-elle aux exigences de la loi ? », *Gaz. Pal.*, 19-20 juillet 2000, p.1280.

BLANC-JOUVAN (G.)

- « Fasc. 321 : Fourniture d'un logiciel ou d'un progiciel», *LexisNexis*, 20 Avril 2009, n°17 et s.

BOURETZ (E.)

- « La défaillance de la régulation financière », *Revue de Droit bancaire et financier* n° 5, Septembre 2009, dossier 26, n°12.

BOURGEOS-BONNARDOT (C.)

- « Fasc. 2750 : Régime Juridique des Archives », 27 Avril 2010, date de la dernière mise à jour : 28 Août 2014, *JurisClasseur Communication*.

BOUTEILLER (P.)

- « Fasc. 765 : Gage Warrant », 6 Avril 2016, *JurisClasseur Banque - Crédit – Bourse*

BOYADJIAN (J.)

- « La science politique face aux enjeux du « *big data* » et de la protection des données personnelles sur internet », *RD pub*. 2016, n° 1, p. 7.

CACHARD (O.) :

- « Le domaine coordonné par la directive sur le commerce électronique et le droit international privé », *RDAI*, 2004.

- « Définition du commerce électronique et loi applicable », *Com. com, élec*., 2004.

CAPRIOLI (E.) :

- « Ecrit et preuve électronique dans la loi n◦2000-230 du 13 mars 2000 », *JCP* éd. E, 2000, suppl. n◦30, p.2.

- « La loi-type de la CNUDCI sur les signatures électroniques », *Com. com, élec*., décembre 2001, chron., 27.

- « La validité du contrat par voie électronique dans le projet de la loi pour la confiance dans l'économie numérique », *Journal des sociétés*, décembre 2003, n◦5, p.4, La revue de l'Avocat Conseil d'Entreprises, n◦86, 2003.

- « *la sincérité de la signature électronique* », *in* O. Le Bot (sous la coordination), *la sincérité en droit, Bruxelles, Larcier*, 2011, p. 111-127, [En ligne: http://www.caprioli-avocats.com/publications/54-dematerialisation-archivage/246-la-sincerite-de-la-signature-electronique].

- « Le crédit documentaire face aux technologies de l'information », *Revue de Droit bancaire et financier n.1*, janvier 2008, dossier 6 – *Le crédit documentaire* en 2008 – *LexisNexis SA*.

- « La confiance dans l'économie numérique », *Petites Affiches* du 3 juin 2005, p. 4.

CAPRIOLI (E.) et AGOSTI (P.)

- « La régulation du marché européen de la confiance numérique : enjeux et perspectives de la proposition de règlement européen sur l'identification électronique et les services de confiance », *Com. com, élec*. n° 2, Février 2013, étude 3, n°12.

CATALA (P.) :

- « L'engagement électronique de l'entreprise », *Revues des sociétés* 2001 p.258, Éd. Dalloz 2011.
- « Le formalisme et les nouvelles technologies », *Defrénois* 2000, art. 37210, p. 897.

COSTES (L.) :

- « Un nouveau cadre juridique pour les communications électroniques », *Cahier Lamy Droit de l'information et des réseaux*, juin 2004, n◦ 170, p.1.

COUTENIER

- « Les techniques de mobilisation des créances internationales - Aspects de droit international et de droit comparé », *RD aff. int.* 3/1999, p. 295.

DELBECQUE (Ph.)

- « Transport maritimes. Travaux de la CNUDCI. Projet d'instrument sur le transport de marchandises par mer », *RTD Com.* 2003 p. 849. *Éd. Dalloz* 2011.

DESCHANEL (J.-P.)

- « Fasc. 440 : Lettre de change relevé (LCR) Billet à ordre relevé », *jurisClasseur Banque - Crédit – Bourse*, 15 Juillet 1999, mise à jour le 27 Novembre 2015.

DOUVRELEUR (O.)

- « Le soft law en matière financière : le point de vue de l'Autorité des marchés financiers », *Revue de Droit bancaire et financier* n° 1, Janvier 2012, dossier 5.

DROSS (W.)

- « Fasc. unique : Prescription Acquisitive – Possession », *JurisClasseur Civil Code*, 20 Février 2013, n°9.

FAUCHOUX (V.) et DEPREZ (P.)

- « Le droit de l'Internet », *LexisNexis SA*, 2008, n°3

FERAL-SCHUHL (C.)

- Les apports du droit de l'informatique et des nouvelles technologies, dix risques à anticiper dans les contrats : *Dr. et patrimoine* 3/2003, p. 59.

GABRIEL (H.)

- « Warehouse Receipts and Securitization in Agricultural Finance », *Revue de droit uniforme*, 2012, p. 369.

de GAUDEMAR (H)

- « La preuve devant le juge administrative », *Droit Administratif* n° 6, Juin 2009, étude 12, *LexisNexis*, n°10 et s.

GAUTRAIS (V.) :

- « Afin d'y croire – Guide relatif a la gestion des documents technologiques », Edition *Fondation du Barreau du Québec*, Novembre 2005.
  [En ligne: http://www.fondationdubarreau.qc.ca/pdf/publication/Guidetech_FR.pdf].

GAUTRAIS (V.) et PORCIN (A.)

- *« Les 7 péchés de la L.p.c. : actions et omissions applicables au commerce électronique»*, (2009) 43 *R.J.T.* 559., disponible en ligne sur le lien suivant : https://ssl.editionsthemis.com/uploaded/revue/article/18343_gautrais.pdf

GIBIRILA (D.)

- « Fasc. 760 : Suretés Portant sur des Biens », *JurisClasseur Banque - Crédit – Bourse*, 1er Août 2008, date de la dernière mise à jour : 27 Mai 2014. © *LexisNexis SA.*

GOBERT (D.)

- « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », février 2015, dossier publié sur le site http://www.droit-technologie.org.

GOBERT (D.) et MONTERO (E.) :

- « L'ouverture de la preuve littérale aux écrits sous forme électronique », *Journal des Tribunaux*, 2001, N◦115, p.117.

GRYNBAUM (L.) :

- « Fasc. 10 : La Preuve Littérale - Dispositions générales - Écrit électronique », *LexisNexis*, 19 Décembre 2011, mise à jour le 17 Juin 2016.

- « Loi confiance dans l'économie numérique » : une version définitive proche de la version originale de la Directive « Commerce électronique », *Com. com. élect.*, 2004, commentaires, p.38.

HARICHAUX (M.)

- « La télétransmission des feuilles de soins », *Revue de droit sanitaire et social* 1998 p.496, *Éditions Dalloz* 2011.

HOVASSE (H.)

- « Fasc. 2030 : Warrants financiers », *JurisClasseur Banque - Crédit – Bourse*, 1er Août 2012.

HUET (J.) :

- "*Fasc. 2420 : Pratiques des Contrats Électroniques*", 26 Mai 2014, Date de la dernière mise à jour en 27 Juillet 2014, *JurisClasseur Contrats – Distribution*, *LexisNexis*.
- « vers une consécration de la preuve et de la signature électroniques », *Éditions Dalloz* 2011, p.95.

- « Encore une modification du Code civil pour adapter le droit des contrats à l'électronique », *JCP G* 2004, I, 178.

- « Le droit applicable dans les réseaux numériques », in *Le droit international de l'Internet*, actes du Colloque organisé à Paris les 19 et 20 novembre 2001 par le Ministère de la justice, l'Université Paris I et l'Association *ARPEJE, Bruxelles, Bruylant*, 2002, p. 71.

- « Aspects juridiques de l'EDI, Échanges de Données Informatisées - *Electronic Data Interchange* », *D. 1991, chron. 181*.

HUON (PH.)

- Droit Uniforme en Droit du Commerce International, [En ligne : http://www.memoireonline.com/01/08/866/m_droit-uniforme-droit-commerce-international4.html**].**

Lescot (P.) et Roblot (R.)

- « Fasc. 2505 : Redressement et Liquidation Judiciaires. – Nullités de droit. – Régime des paiements », *JurisClasseur Droit international*, © *LexisNexis SA*, 1 Juil. 2001.

LANNA (M.)

- « Le quantified-self, nouveau moteur du *big data* et menace pour la vie privée », LPA 12 mai 2016, n° 95, p. 6.

LASSALAS (CH.)

- « Fasc. 550 : Escompte », 1er Janvier 2016, *JurisClasseur Banque - Crédit – Bourse*.

LIGHTBURN (J.) & NATAF (Ph.)

- « La loi portant adaptation du droit de la preuve aux technologies de l'information », *la Semaine Juridique Entreprise et Affaires* n. 21, 25 mai 2000, p.836, *Lexis-Nexis* SA.

LIKILIMBA (Guy-Auguste)

- « La possession corpore alieno », *RTD Civ*. 2005.

LUBY (M.)

- « Protection des consommateurs. Commerce électronique. Commerce sur Internet », (Déc. n. 276 du 25 janv. 1999, *JOCE* L. 33 du 6 févr. 1999), *RTD Com*. 1999 p.811, 2 pages, *Éd. Dalloz* 2011.

MARINO (L.)

- « Notre vie privée : des little data aux *big data*, Le secret dans la vie des personnes », in Le secret à l'ère de la transparence : *JCP E* 2012, suppl. n° 47, p. 14.
- « Le big data bouscule le droit », *RLDI* déc. 2013, n° 3300.

MATHIAS (J.-D.) :

- « l'authenticité électronique », in *Vers l'authenticité électronique*, Dixième rencontres notariat-université, chambre interdépartementales des notaires de Paris, 11 déc. 2000, *Les Petites Affiches*, 2 av. 2001, n◦ 65, p.25.

PASSANT (E.) :

- « La loi du 13 mars 2000, portant adaptation du droit de la preuve aux nouvelles technologies et relative a la signature électronique : une nouvelle donne pour le droit de la preuve », *Cahier Lamy Droit de l'informatique et des réseaux*, mai 2000, n◦125, p.8.

- « Le décret du 31 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique », *Cahier Lamy Droit de l'informatique et des réseaux*, juin 2001, n◦137, p.2.

LUPOVICI (C.)

- « Les stratégies de gestion et de conservation préventive des documents électroniques », *BBF* 2000 Paris.

MOULY-GUILLEMAUD

- « La sentence "nul ne peut se constituer de preuve à soi-même", ou le droit des preuves à l'épreuve de l'unilatéralisme », *RTD civ. 2007, p. 253 et s., note 18.*

PERRAY (R.)

- « Fasc. 274-10 : « Informatique - Données à caractère personnel - Introduction générale et champ d'application de la loi "Informatique et libertés" », *JurisClasseur Administratif, LexisNexis*, 18 Mai 2016, Date de la dernière mise à jour : 19 Octobre 2016.

PIETTE-COUDOL (Th.) :

- « Fasc. 80 : Les Collectivités Territoriales Face aux Technologies de l'Information et de la Communication », *LexisNexis*, 24 Octobre 2014, p. 8 et s.

- « Fasc. 60-58: Dématérialisation des procédures », *JurisClasseur Contrats et Marchés Publics*, 1 Octobre 2011© *LexisNexis SA.*

PIRONON (V.)

- « Dits et non-dits sur la méthode de la focalisation dans le contentieux - contractuel et délictuel - du commerce électronique », *Journal du droit international* (Clunet) n° 4, Octobre 2011, var. 4.

PLANTEY (A.) et PLANTEY (M.-C.)

- « Fasc. 111 : Prescription Quadriennale – Domaine, maniement, effets, contentieux », *LexisNexis* 16 Juillet 2014, n°17.

POIDEVIN (B.) :

- « Le cadre juridique de la certification », 1er sept. 2002, disponible en ligne sur le site http://www.juriscom.net, p. 1 et 2.

RAYNOUARD (A.) :

- « Adaptation du droit de la preuve aux technologies de l'information et à la signature électronique, observations critiques », *Defrénois*, 2000, n◦10, p.593.

- « Le droit de l'écrit électronique », *Les Petites Affiches*, 1 avr. 2001, n◦65, p.15.

RENARD (I.):

- « 3 QUESTIONS Le Cloud Computing », *La Semaine Juridique Entreprise et Affaires* n° 50, 13 Décembre 2012, 770.

ROCHFELD (J.)

- « Accomplissement de certaines formalités contractuelles par voie électronique – Ordonnance n. 2005-674 du 16 juin 2005 », (*JO* 17 juin 2005, p. 10342), *RTD Civ*. 2005 p. 843, *Éd. Dalloz* 2011.
- « La loi n. 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique », *(JO* 22 juin 2004, p. 11168), *RTD Civ*. 2004 p.574, *Éditions Dalloz*.
- « Loi n. 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique », (*JO* 14 mars 2000, p. 3968), *RTP Civ*. 2000 p. 423, *Éd. Dalloz* 2011.

ROBLOT (R.)

- « Fasc. 425 : Lettre de Change – Acceptation », *JCP, 2 Juin 2014 © LexisNexis SA.*

SORDET (E.) et MILCHIOR (R.)

- *« Le Cloud computing, un objet juridique non identifié ? », Com. com. élec. n° 11, novembre 2011, étude 20.*

SCHAPIRA ET LEBEN

- *Le droit international des affaires* : *PUF, 5e éd. 1996, Coll. Que sais-je ?, n° 1465*

SCHWERER (F.) :

- « Réflexions sur la preuve et la signature dans le commerce électronique », *Com. com. élec.*, déc. 2000, *chron*., p.4.

SEDALLIAN (V.) :

- Les problèmes posés par la législation française en matière de chiffrement, Droit de l'Informatique et des télécoms 98/4 (10/98) [En ligne : http://encryption_policies.tripod.com/france/sedallian_1098_prob.htm

- « Preuve et signature électronique », oct. 2000, disponible en ligne sur le site : http://www.juriscom.net/chronique.

- « *L'archivage de l'acte électronique* », *Cahier Lamy Droit de l'informatique et des réseaux*, juil. 2002. n◦149, p.1.

SEUBE (E.) :

- « Les conditions générales des contrats », in *Mélanges A. JAUFFRET*, Faculté de droit et de science politique d'Aix-Marseille, 1974, p.662.

SOSINSKY (B.)

- Cloud Computing Bible, *John Wiley & Sons*, January 11, 2011, p.17 et s.

SORDET (E.) et MILCHIOR (R.)

- « Le Cloud computing, un objet juridique non identifié ? », *Communication Commerce électronique* n° 11, Novembre 2011, étude 20.

SOUSI (B.)

- « L'adaptation du droit bancaire et financier européen aux nouvelles technologies », *RJ com*. 2001, p. 77.

STOUFFLET (J.)

- « Fasc. 1080 : Crédit Documentaire », 10 Novembre 1998, Date de la dernière mise à jour : 27 Septembre 2015, JurisClasseur Banque - Crédit – Bourse, *LexisNexis*, n°40 et s

SCHVIKA

- « Du déclin de la négociabilité des instruments de paiement et de crédit », *D.* 2000, chron

THOMAS (V.)

- « Fasc. 566-20 : Effets de Commerce. - Lettre de change et billet à ordre. – Warrant », JCP 30 Oct. 2002, n° 14.

TRÉBULLE (F.-G.) :

- « La reforme du droit de la preuve et le formalisme », *Les Petites Affiches*, 20 avr. 2000, n◦79, p.10.

- « Fasc. 160: Incidence de la réforme de la preuve sur le droit bancaire », *JurisClasseur Banque - Crédit – Bourse*, 15 Avril 2000, © *LexisNexis SA.*

TRUCHE (P), FAUGÈRE (J.P.), FLICHY (P.)

- « Administration électronique et protection des données personnelles » *Livre Blanc*, [En ligne : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000100/0000.pdf], consulté le 26 mars 2016.

ULDALL (R.) et de MONTIS (W.),

- « Réforme sur la protection des données: le Parlement approuve de nouvelles règles adaptées à l'ère numérique», 14 Avril 2016, [En ligne : http://www.europarl.europa.eu/]

VAN OVERSTRAETEN (T.) :

- « Droit applicable et juridiction compétente sur Internet », *RDAI*, 1998, p.383.

VASSEUR (M.)

- « La lettre de change-relevé. De l'influence de l'informatique sur le droit », *RTD com*. 1975, p. 203

VIVANT (M.) :

- « Un projet de loi sur la preuve pour la société de l'information », *Cahier Lamy Droit de l'Informatique et des réseaux*, 1999. *Bulletin d'actualité*, 1999, Fascicule E, n°117, p.9.

WARUSFEL (G.) :

- « Aspects juridiques de la dématérialisation des échanges dans le commerce électronique », in Internet, commerce et droit : vers un droit de l'économie numérique, Colloque Université Paris 5-René Descartes, le 21 mars 2003, *Les Petites Affiches*, 6 fév. 2004.

WERY (E.) :

- « Les phénomènes d'autorégulation sur le Web », in *Les premières journées internationales du droit du commerce électronique, Colloque, Nice*, 23-25 Octobre 2000, *Litec*, 2000.

STUBBS (E.) :

- « *Big Data Big Innovation – Enabling Competitive Differentiation through Business Analytics*», edition John Wiley & Sons 2014, 232 pages.

ZOLA (M.) :

- « La notion de consentement à l'épreuve de l'électronique (2ème partie) », *Gaz. Pal.*, 14 au 16 oct. 2001, p.1133.

IV. CHRONIQUES

Groupes de travail au sein de la Commission des Nations Unies pour le droit commercial international

- « Questions juridiques liées à l'utilisation des documents transférables électroniques », '*A/CN.9/WG.IV/WP.115*', Commission des Nations Unies pour le droit commercial international, Groupe de travail IV (Commerce électronique), Vienne, 10-14 octobre 2011.

- « *Travaux actuels et travaux futurs possibles dans le domaine du commerce électronique* », A/CN.9/692. Commission des Nations Unies pour le droit commercial international – Quarante-troisième session, New York, 29 juin-9 juillet 2010 – 18 pages.

- « *Travaux actuels et travaux futurs possibles dans le domaine du commerce électronique* », A/CN.9/728/Add.1. Commission des Nations Unies pour le droit commercial international, Vienne, 27 juin-15juillet 2011 – 16 pages.

- « *Aspects juridiques du commerce électronique – Proposition du Gouvernement espagnol* »; A/CN.9/WG.IV/WP.116. Commission des Nations Unies pour le droit commercial international – Groupe de travail IV (Commerce électronique) Quarante-cinquième session, Vienne, 10-14 Octobre 2011 – 9 pages.

- « *Ordre du jour provisoire annoté* », A/CN.9/WG.IV/WP.114. Commission des Nations Unies pour le droit commercial international – Groupe de travail IV (Commerce électronique) Quarante-cinquième session, Vienne, 10-14 Octobre 2011 – 6 pages.

- « *Travaux futurs envisageables sur le commerce électronique – Transfert de droits sur les biens corporels et autres droits* », A/CN.9/WG.IV/WP.90. Commission des Nations Unies pour le droit commercial international – Groupe de travail sur le commerce électronique Trente-huitième session, New York, 12-23 mars 2001 – 33 pages.

- *« Droit des transports : élaboration d'un projet d'instrument sur le transport de marchandises {effectué entièrement ou partiellement par mer} Proposition de révision des dispositions sur le commerce électronique »*, A/CN.9/WG.III/WP.47, Commission des Nations Unies pour le droit commercial international – Groupe de travail III (Droit des transports) Quinzième session, New York, 18-28 avril 2005 – 13 pages.
- « Commerce électronique et services de transports internationaux », Conférence des Nations Unies sur le commerce et le développement (CNUCED), 'TD/B/COM.3/EM.12/2', 31 Juillet 2001.

V. Conventions Internationales et Législations nationales et internationales.

A. Conventions Internationales

- *Loi type de la CNUDCI sur les signatures électroniques, 5 juillet 2001, Publication des Nations Unies, New York,* 2002.

- *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation 1996, Publication des Nations Unies, New York,* 1999.

- *Convention portant loi uniforme sur les lettres de change et billets à ordre, Genève*, 7 juin 1930. [En ligne : https://treaties.un.org/].

- *Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux, Publication des Nations Unies, New York,* 2007.

- *Convention des Nations Unies sur les lettres de change internationales et les billets à ordre internationaux, Publication des Nations Unies, New York,* 1988.

- *Convention portant loi uniforme sur les lettres de change et billets à ordre (Convention de Genève), Genève*, 7 juin 1930.

- *Les nouvelles Règles et Usances uniformes de la Chambre de Commerce Internationale (CCI) relatives aux crédits documentaires (Révision 2007), en abrégé RUU 600,* entrent en vigueur le 1er juillet 2007

- *Convention des Nations Unies sur le contrat de transport international de marchandises effectué entièrement ou partiellement par mer (les "Règles de Rotterdam")*, adoptée par l'Assemblée générale le 11 décembre 2008, *Publication des Nations Unies, Vienne*, 2009.

- *Convention relative aux garanties internationales portant sur des matériels d'équipement mobiles, Le Cap*, 16 nov. 2001 (*la Convention du Cap*). [En ligne : http://www.unidroit.org/french/conventions/mobile-equipment/mobile-equipment.pdf].

- *Directive Européenne n°2001-29 du 22 mai 2001 2001/29/CE DU PARLEMENT EUROPEEN ET DU CONSEIL du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, Journal officiel* n° L 167 du 22/06/2001 p. 0010 - 0019.

- *Convention des Nations Unies sur les contrats de vente internationale de marchandises en date de 11 avril 1980, Publication des Nation Unies, New York,* février 2011.

- *Directive du 24 octobre 1995/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à*

caractère personnel et à la libre circulation de ces données. [En ligne : http://data.europa.eu/eli/dir/1995/46/oj].

- *Directive n°1999/93/ CE du Parlement et du Conseil, 13 déc. 1999, sur un cadre communautaire pour les signatures électroniques, Journal Officiel des communautés européennes*, 19 janv. 2000. [En ligne : http://data.europa.eu/eli/dir/1999/93/oj].

- *Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, Journal officiel* n° L 144 du 04/06/1997 p. 0019 - 0027.

- *Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE*. [En ligne : http://data.europa.eu/eli/reg/2014/910/oj].

- *Proposition de Règlement du Parlement européen et du conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, Bruxelles, 4 juin 2012*, [En ligne : http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com%282012%290238_/com_com%282012%290238_fr.pdf].

- *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).* [En ligne : http://data.europa.eu/eli/reg/2016/679/oj].

- *Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information* (Texte présentant de l'intérêt pour l'EEE). [En ligne : http://data.europa.eu/eli/reg/2004/460/oj].

- *Pacte international relatif aux droits civils et politiques de 1966, Onu,* 16 décembre 1966. [En ligne : http://www.assemblee-nationale.fr/].

- *La Déclaration universelle des droits de l'homme de 1948, Onu,* 10 décembre 1948. [En ligne : http://www.un.org/].

B. Législations Nationales

Lois

- *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1)*, version consolidée au 15 novembre 2016. [En ligne : http://www.legifrance.gouv.fr/].

- *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, *JO* du 22 juin 2004.

- *Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*, *JO* du 14 mars 2000, p. 3968.

- *Loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées. Journal Officiel 16 Mai 2009.*

- *Loi n° 2008-561, 17 juin 2008 portant réforme de la prescription en matière civile*, *JO* 18 juin, p.9856.

- *Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, Journal Officiel* 13 Juillet 1991.

- *Loi n° 2004-801, 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Journal Officiel* 7 Aout 2004.

- *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (dite "Loi informatique et libertés"), Journal officiel* du 7 janvier 1978 et rectificatif *au J.O.* du 25 janvier 1978.

- *Loi du 29 juillet 1881 sur la liberté de la presse*, version consolidée au 29 janvier 2014 : [En ligne : http://www.legifrance.gouv.fr/].

Arrêtés

- *Arrêté du 20 avril 2016 portant approbation du référentiel général d'interopérabilité.* [En ligne : https://www.legifrance.gouv.fr/eli/arrete/2016/4/20/PRMJ1526716A/jo/texte].

- *Arrêté du 20 avril 2011 relatif à la reconnaissance de la qualification des prestataires de services d'horodatage électronique et à l'accréditation des*

organismes qui procèdent à leur évaluation, JORF n°0094 du 21 avril 2011 page 7094.

- *Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques*. [En ligne: https://www.legifrance.gouv.fr/eli/arrete/2014/6/13/PRMD1413745A/jo/texte].

- *Arrêté du 6 mai 2010, portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certifications électroniques : Journal Officiel* 18 Mai 2010.

- *Arrêté du* 27 *juin 2007 portant application de l'article D. 1617-23 du Code général des collectivités territoriales relatif à la dématérialisation des opérations en comptabilité publique : Journal Officiel* 11 Juillet 2007.

- *Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation, JO* 8 juin, p. 10223.

- *Arrêté du 22 décembre 1981 portant enrichissement du vocabulaire informatique, JO* 10 no. 1984.

- *Arrêté du 4 janvier 2002 modifiant l'arrêté du 17 mars 1992, Journal Officiel* 5 Février 2002.

- *Arrêté du 22 décembre 1981 portant enrichissement du vocabulaire informatique, JO* 10 no°1984.

Ordonnances

- *Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*, version consolidée au 20 novembre 2016. [En ligne : http://www.legifrance.gouv.fr/].

- *Ordonnance n° 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique, Journal Officiel* du 17 Juin 2005.

- *Constitution de 1946, IVe République,* 27 octobre 1946. [En ligne : http://www.conseil-constitutionnel.fr/].

- *Constitution du 4 octobre 1958*, version consolidée au 1 janvier 2015. [En ligne : http://www.conseil-constitutionnel.fr/].

- *Code Civil*, version consolidée au 9 octobre 2016. [En ligne : https://www.legifrance.gouv.fr/].

- *Code de Commerce*, version consolidée au 20 octobre 2016. [En ligne : https://www.legifrance.gouv.fr/].

- *Code de la Consommation*, version consolidée au 10 octobre 2016. [En ligne : https://www.legifrance.gouv.fr/].

- *Code rural et de la pêche maritime*, version consolidée au 3 décembre 2016. [En ligne : https://www.legifrance.gouv.fr/].

Décrets

- *Décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat, JORF n°0094 du* 21 avril 2011 page 7093

- *Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information*, version consolidée au 07 août 2016. [En ligne : https://www.legifrance.gouv.fr/].

- *Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* version consolidée au 20 novembre 2016. [En ligne : https://www.legifrance.gouv.fr/].

- *Décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie,* version consolidée au 20 novembre 2016. [En ligne : https://www.legifrance.gouv.fr/].

- *Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Journal Officiel 4 Février 2010, p. 2072.* [En ligne: https://www.legifrance.gouv.fr/eli/decret/2010/2/2/PRMX0909445D/jo/texte].

- *Décret n° 2001-272, 30 mars 2001, pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique, JO* 31 mars 2001, p. 5070.

- *Décret n° 2002-535, 18 avril 2002, relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, JO* 19 avril 2002, p. 6944.

- *Décret n°2009-302 du 18 mars 2009 portant application de l'article L. 132-1 du code de la consommation, détaillant la loi n°2008-776 du 4 août 2008 de modernisation de l'économie.*[Enligne:https://www.legifrance.gouv.fr/eli/decret/2009/3/18/ECEC0829592D/jo/texte].

C. Législations Américaines

- *Uniform Electronic Transactions Act (UETA)* in 1999 - la Loi uniforme sur les opérations électroniques de 1999 (UETA).

- *US Uniform Commercial Code (UCC)* (le Code de Commerce Uniforme).

- *US federal Electronic Signatures in Global and National Commerce Act,* June 30, 2000.

VI. Jurisprudence étatique et notes de Jurisprudence

- Tribunal de Grande Instance de Paris, Ordonnance de référé du 14 aout 1996, RG n° 60139/96 Société Art Music France et a. c/ ENST et a. *Dalloz* 2015.

- Tribunal de Grande Instance de Paris, Ordonnance de référé du 14 aout 1996, Société Editions musicales Pouchenel et a. c/ Ecole Centrale de Paris (ECP) et a. *Dalloz* 2015.

- Cass.com., 2 juin 2015, n° 14-13.775, FS-P+B, M. X c/ Banque populaire des Alpes : *JurisData* n° 2015-013154; *JCP E* 2015, 1466, note Rodriguez : *RD bancaire et fin*. 2015, *comm.* 179, obs. Francis-J. Crédot et Th. Samin.

- Com. 30 oct. 2012, n° 11-23519, *Bull.* n° 195; *Gaz. Pal.*, 12 déc. 2012, chron. 12, n. Dumont-Lefrand

- Com. 9 mars 1999, *RTD com*. 1999. 929, obs. Cabrillac; *RDBF* 1999. 94, obs. Crédot et Gérard

- Com. 13 mai 1996, *Bull. Civ*. IV, n°88.

- Com. 13 janv. 1982, *JCP* 1982. IV. 114.

- Com. 29 nov. 1994, *Bull*. n° 353; *RTD com*. 1995. 173, obs. Cabrillac: tirage par le cédant Dailly pour compte du cessionnaire, après notification de la cession; le tiré accepteur peut être des lors oppose le défaut de provision au donneur d'ordre (cessionnaire de la créance) qui n'a pas la qualité d'un tiers porteur.

- Com. 10 mars 1970, *Bull. Civ. IV*, n°91 rejetant un pourvoi contre Paris, 24 janv. 1968, *RTD com*, 1969. 130, obs. Cabrillac et Rives-Lange.

- Com. 13 sept, 2011, n°10-19963, *Bull.* n°129; *D.* 2011, act. 2269, obs. Delpech; *JCP G* 2011. 1046, obs. Lasserre Capedeville ; *Banque et Dr.* Nov. 2011, 15 obs. Bonneau ; *Gaz. Pal.*, 28 oct. 2011. 31, n. Houin-Bressand.

- Comp. Com. 18 janv. 1994, *RJDA* 1994. 540.

- Paris, 14e ch. B, 26 sept. 1997 : *D*. 1997, inf. Rap. O.221. – Paris 3e ch. C, 20 Janv. 1995: *D*. 1996, *somm*. P. 34, obs. Cabrillac).

- Com. 13 sept. 2011, no10-19.963, *Bull.* no 129; D. 2011. 2269, n. Delpech; *JCP G* 2011.1750, n. Lasserre Capdeville; *Gaz. Pal.*, 28 oct. 2011. 31, n. Houin-Bressand ; *Banque et Dr*. nov. 2011. 15, obs. Bonneau ; *Dalloz* actualité 22 Sept. 2011 ; *RD bancaire et fin*. Nov.-déc. 2011, obs. Crédot et Samin).

- Rennes, 1er ch. B, 14 déc. 2007, *RG* no 06/07107, Basle c/ Credit mutuel de Rohan Réguiny, *Juris-Data* no 357288.

- Renne, 1e ch. B, 22 juin 2006, IV, 3467.

- Rouen, 14 juin 1963, *D*. 1963.636 ; Banque 1963.866, obs. Marin, V. Ss no517.

- T. com. Lyon, 9 févr. 1970 : *Banque 1970, p. 816, obs. X. Marin ; RTD com. 1970, p. 750, n° 1, obs. M. Cabrillac et J.-L. Rives-Lange.*

- Com. 30 oct. 2012, no 11-23519, *Bull.* no 195; *Gaz. Pal.*, 12 déc. 2012, chron. 12, n. Dumont-Lefrand; *Banque et Dr*. Nov. 2012. 54, n. Jacob ; RLDA déc. 2012. 30, n. Mauriès ; *RTD com*. 2013. 124, obs. Legeais.

- Com. 9 mai 1962, *Bull. civ. III*, no 247. Com. 7 nov. 1979, *Gaz. Pal.* 1980. 1.44, note J.D.; *RTD com*. 1980. 115, obs. Cabrillac et Rives-Lange.

- Com. 29 juin 1983, Bull. civ. IV, no 198. Com. 13 mars 1985, *Bull. civ. IV*, no97; *D.* 1985. IR. 418, obs. Cabrillac. Com. 7 oct. 1987, *D.* 1988. *Somm*. 51, obs. Cabrillac.

- Amiens, 15 oct. 1993 : *JCP* 1994. II. 22258, note *Mossot-Durin*.

- CA. Besancon, ch. Soc., 20 oct. 2000, Chalets Boisson c/Gros, Expertises févr. 2001. P.73, note Beaujard ; CCE janv. 2001, p.22, note Galloux ; *JCP* 2000, II, 10606, note Caprioli et Agosti – Confirmée par Civ. 2e, 30 avr. 2003, n.00-46.467, *Bull.civ* II, n.118.

- Cass. 1er civ., 21 déc. 1964: *Bull. civ. 1964, I, n° 589. - Cass. 3e civ., 8 mai 1969: Bull. civ. 1969, III, n° 371.*

- Cass. 1er civ., 7 févr. 1962: *Bull. civ. 1962, I, n° 91. Dans ce sens,* le fait d'avoir pris certaines terres à bail n'interdit pas en principe au fermier de bénéficier de la présomption édictée par l'article 2256 à propos de parcelles non comprises dans le bail *(CA Caen, 26 mai 1998, n° 9601948 : JurisData n° 1998-045926).*

- Cass. 1er civ., 25 févr. 1963: *Bull. civ. 1963, I, n° 119. - Cass. 3e civ., 18 mars 1970 : Bull. civ. 1970, III, n° 219.*

- Cass. 3e civ., 18 déc. 2002, *n° 01-12.143: JurisData n° 2002-017037; Bull. civ. 2002, III, n° 261 ; RTD civ. 2003, p. 319, obs. Th. Revet ; RTD civ. 2003, p. 327, obs. P. Crocq*

- Décision n° 71-44 DC du 16 juillet 1971 : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1971/71-44-dc/decision-n-71-44-dc-du-16-juillet-1971.7217.html

- Décision du Conseil constitutionnel n° 2000-433 DC du 27 juillet 2000 modifiant la Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication. http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=8451AEF6764B35C1295707CA9DDDA8CA.tpdjo08v_2&dateTexte=?cidTexte=JORFTEXT000000583643&categorieLien=cid

VII. Sites Internet

- http://www.legifrance.gouv.fr/

- http://www.legislation.gov.uk/

- http://www.assemblee-nationale.fr

- http://www.zeblogsante.com/web-3-0-definition/

- https://www.whitehouse.gov/

- http://www.un.org/fr/

- http://www.crdp-montpellier.fr/

- http://www.humanrights.ch/fr/

- https://www.cnil.fr/

- http://www.europarl.europa.eu/

- http://eur-lex.europa.eu/

- http://www.cours-de-droit.net/

- http://www.memoireonline.com/

- *www.uncitral.org*

- *http://www.larousse.fr*

- http://www.ssi.gouv.fr/

- http://www.bbc.co.uk/

- https://www.securiteinfo.com
- http://encryption_policies.tripod.com
- http://www.wefightcensorship.org
- http://www.internet-juridique.com
- http://www.dictionnaire-juridique.com/
- http://www.textes.justice.gouv.fr/
- https://treaties.un.org/
- http://searchdatacenter.techtarget.com/
- http://www.vulgarisation-informatique.com/disque-dur.php/
- http://searchstorage.techtarget.com/
- http://www.commentcamarche.net/
- http://www.cisco.com/
- https://blogs.technet.microsoft.com
- http://windows.microsoft.com/
- htttp://ww.interpares.org
- https://www.nist.gov/
- http://www.iso.org/
- http://www.doi.org/
- http://www.indicare.org/
- http://copyright.gov/
- http://www.avae-vvba.be/
- http://www.ago-sa.fr/
- http://www.arcalys.com/
- http://www.ariadne.ac.uk/
- http://www.linternaute.com/
- http://www.aiim.org
- http://www.lenouveleconomiste.fr/

INDEX ALPHABETIQUE

Les chiffres renvoient aux numéros de pages

W

Table des Matières

Résumé

L'intérêt de la présente recherche est d'étudier d'une manière générale les communications électroniques dans le commerce international, et puis à titre particulier d'interpeler les nouveaux défis qui relèveraient de l'utilisation des "documents transférables électroniques", en réfléchissant sur les différentes approches et les méthodes à adopter afin de remédier aux éventuelles déficiences technologiques, identifier puis combler les lacunes juridiques qui se révéler lors de ces échanges.

Il s'agirait donc d'une enquête sur les questions juridiques liées à la création, à l'utilisation et à l'exécution du "document transférable électronique" ; il s'agit d'un terme crée par la CNUDCI, ce qui renvoie d'une manière générale à l'équivalent électronique d'un instrument transférable négociable ou d'un document titre.

Nous identifions principalement les trois grands axes suivants :

I – La protection des données personnelles : Elle fait l'objet de plusieurs réformes législatives. La plus récente est le Règlement européen 2016/679 du 27 avril 2016 qui vise à promouvoir l'utilisation de l'outil informatique, tout en accordant la protection appropriée aux données à caractère personnel.

II – Exigence d'unicité d'un document transférable (« Garantie de singularité ») : La garantie de l'unicité d'un document exige qu'il soit le seul qui existe ou bien, que toute copie soit clairement identifiable comme telle. Les conséquences éventuelles de la reproduction non autorisée de tout document transférable électronique donnant au porteur ou au bénéficiaire le droit de demander la remise de marchandises ou le paiement d'une somme d'argent rendent nécessaire l'élaboration de mécanismes pour garantir l'unicité de ces instruments.

III - La possession du 'document transférable électronique' et la notion de contrôle pour l'identification du porteur : Outre le traitement de la question de l'exigence de la singularité, la recherche d'un mécanisme fonctionnellement applicable et équivalent pour satisfaire à l'exigence de la possession matérielle du document papier constitue un défi majeur. Dans la plupart des modèles juridiques régissant les documents transférables électroniquement, la notion de "contrôle" d'un document électronique est utilisée en tant qu'équivalent fonctionnel de la possession ; cela signifie que la personne qui exerce le contrôle du document transférable électronique est considérée comme le porteur habilité à s'en prévaloir. Ces documents électroniques sont gérés par des prestataires de confiance qualifiés pour garantir leur sécurité.

Summary

The interest of this research is to study in general, the electronic communications in an international context, and then to focus on the ongoing challenges that occur on the field of "electronic transferable documents"; for this we shall perceive the methods that have been adopted for the purpose of using such documents, in order to prevent eventual technological deficiencies, identifying and filling the legal gaps revealed throughout our study of these new challenges.

Therefore we shall comprehend and defy the legal boundaries, in order to create, use and execute an 'electronic transferable document'; this term has been created by UNCITRAL, which refers generally to ' Electronic equivalent of a transferable record (negotiable or non-negotiable) or a document of a legal right.

We shall identify the three following main topics:

I. The protection of personal data and privacy has been subject to several legislative reforms. The most recent one is the European Regulation 2016/679 dated April 27th, 2016. This reform aims to promote the use of the IT (Information Technology) tools, while granting the appropriate protection to the personal data. These electronic records are managed by qualified services providers.

II. Requirement for uniqueness of the record ("Guarantee of uniqueness"): The guarantee of the uniqueness of the document is to ensure that there is only one possible holder and owner of that document, as in the case of paper document, and that any copy is clearly identifiable as such. As a result of an unauthorized reproduction of any electronic transferable record, any such holder or beneficiary shall have the right to request delivery of goods or the payment of a certain sum of money; thus the need to insure the uniqueness of these electronic records.

III. The possession of an electronic transferable record and the concept of 'control' to identify the holder: The need to identify a functional equivalent approach to satisfy the requirement of possession while dealing with an electronic transferable record is a major challenge. In most legal models concerned with this subject, the concept "control" is used for transferable electronic records as a functional equivalent to the material possession. That is, the person who controls the electronic transferable record is deemed to be the holder and the one entitled to use it. These electronic records are managed by qualified services' providers to secure the documents.