UNIVERSITÉ PARIS 13 NORD

LE DÉVELOPPEMENT DE LA SIGNATURE ÉLECTRONIQUE

Sous la Direction de Madame le professeur SEBAG

Virginie ETIENNE

Master 2 Recherche Droit des affaires

Dirigé par M. GUÉVEL

Année universitaire 2010-2011

REMERCIEMENTS

Je souhaite adresser ici tous mes remerciements aux personnes qui m'ont apporté leur aide et qui ont ainsi contribué à l'élaboration de ce mémoire.

Je tiens particulièrement à remercier ma Directrice de mémoire, Madame Sebag, pour son soutien, ses conseils et son aide précieuse.

Je remercie le Directeur du Master 2 Recherche Droit des affaires, Monsieur Guével, sans lequel la chance de suivre cette formation enrichissante et l'élaboration de ce mémoire auraient été impossibles.

Je remercie toutes les personnes qui m'ont apporté des aides ponctuelles tout le long de mon travail, sans oublier le soutien de la part de ma famille et de mes amis.

Je remercie enfin le Conseil National des Greffiers des Tribunaux de commerce, sans lequel je n'aurais pu obtenir le 1er prix du Concours des masters ouvert aux étudiants en fin de 3ème cycle dans une Université française sur les thèmes liés aux missions confiées aux greffiers des Tribunaux de commerce.

SOMMAIRE

INTRODUCTION

« *L'homme en face des choses est fatalement porté à en chercher le secret* » et il ne peut « *rester indifférent devant l'univers* [1]»

[1] E. RENAN, *L'avenir de la science*, Flammarion, 1995, p. 91

1. L'impact des **nouvelles technologies** sur les hommes est impressionnant. Le droit s'est adapté à ces nouvelles inventions, il est influencé par la puissance de la science sur la société et sur les Hommes. La société industrielle est une société portée sur l'innovation, la construction, ce qui entraîne incontestablement des impacts. René Savatier précise que « *le droit et les techniques s'enchevêtrent de plusieurs manières*[2] ». En effet, le droit influence la technique et la technique influence le droit.

2. Les juristes sont également adaptés aux changements juridiques dus aux évolutions technologiques. Une nouvelle technologie appelle un questionnement juridique et le cas échéant une modification juridique. Les juristes redoutent le vide juridique, l'absence de règles dans un domaine particulier, fût-ce en raison d'une évolution scientifique ou autre qui ne serait pas appréhendée par la règle de droit. Or, depuis le XIXème siècle, le développement technologique est devenu un défi pour le monde du droit, avec la peur toujours croissante de l'insécurité juridique.

3. L'évolution au cœur de la technologie moderne est l'**informatique**, le développement des relations virtuelles, en dehors de tout support matériel ou écrit, avec l'utilisation de plus en plus croissante des moyens de télécommunication : « *L'intégration des TIC*[3] *dans le monde juridique se traduit par des chantiers de « dématérialisation » ponctuels*[4]. » On assiste de plus en plus à l'abandon du papier pour l'électronique.

4. Les distances géographiques ne sont plus du tout une préoccupation depuis l'**Internet** et le commerce électronique. Les modes de communication ont explosé en quelques années. On constate un besoin de contracter plus vite, pour consommer plus vite et efficacement. Le développement technologique répond à un besoin toujours plus grand de consommer, et de consommer le plus vite possible. C'est la « *dématérialisation du réel*[5] ».

5. Internet est né dans les années 60 et était utilisé au départ à des fins militaires et universitaires. Les informations étaient donc partagées entre des personnes précises. Le

[2] R. SAVATIER, *Les métamorphoses économiques et sociales du droit privé aujourd'hui, seconde série. L'universalisme renouvelé des disciplines juridiques*, Dalloz, 1959, p. 49
[3] Technologies Industrielles et Commerciales
[4] T. PIETTE-COUDOL, *La remise électronique du bulletin de paie*, JCP S., n° 43, 26 oct. 2010, 140, p. 2
[5] P-Y GAUTIER et X. LINANT de BELLEFONDS, *De l'écrit électronique et des signatures qui s'y attachent*, JCP G., n°24, 14 juin 2000, I 236, p. 1, §1

premier grand réseau numérique est né en 1969[6]. Internet est devenu progressivement le « réseau des réseaux[7] », celui qui relie tous les réseaux différents des Etats. D'un rôle uniquement informatif, Internet est devenu un outil de partage et de communication. Il est ensuite devenu un moyen de communication majeur dans la majorité des sociétés d'aujourd'hui. Les trois critères caractérisant Internet que sont la dématérialisation, l'ubiquité et l'interactivité, ont donné naissance au commerce électronique. Il faut savoir aujourd'hui que 70% des Entreprises dans le Monde sont dotées d'un site Internet que ce soit dans un but uniquement informatif ou commercial.

6. Le **commerce électronique** se caractérise par « *l'abolition des distances géographiques et la réduction du temps*[8] ». Il est devenu un enjeu politique et économique majeur dans les pays industrialisés. Internet n'est pas un « *no man's land juridique*[9] » avec le développement de règles juridiques transnationales en matière de commerce électronique et la possibilité de dématérialiser les documents commerciaux depuis plus de vingt ans. L'essor du commerce électronique repose sur la confiance des utilisateurs sur le système. Le droit a dû intervenir pour relever le défi juridique de comprendre les technologies pointues touchant le commerce électronique (le paiement sécurisé en ligne, la définition des obligations du cyber-commerçant…)

7. Dans le monde juridique une personne physique (même morale d'ailleurs) doit s'identifier aux yeux des autres acteurs en déclarant une **identité**: son nom. Toute relation par voie électronique créé des doutes entre les personnes, il n'y a aucune certitude sur l'identité des contractants. Or, la connaissance des identités et de l'engagement dans les relations contractuelles sur internet sont très importants. C'est pourquoi le recours à la signature électronique s'est imposé.

8. Mais tout d'abord, qu'est-ce qu'une **signature** ? Selon le Dictionnaire Robert, la signature est « *une inscription qu'une personne fait de son nom (sous une forme particulière et constante) pour affirmer l'exactitude, la sincérité d'un écrit ou en assumer la responsabilité.* ». Selon C. Devys : la signature est « *tout signe intimement lié à un acte*

[6] L' « Arpanet » aux Etats-Unis.
[7] « Interconnected Networks »
[8] E. A CAPRIOLI, *Sécurité et confiance dans le commerce électronique : signature numérique et autorité de certification*, JCP G., n° 14, 1er avr. 1998, I 123, p. 1, §1
[9] E. A CAPRIOLI, *Sécurité et confiance dans le commerce électronique : signature numérique et autorité de certification*, JCP G., n° 14, 1er avr. 1998, I 123, p. 1, §2

permettant d'identifier et d'authentifier l'auteur de cet acte et traduisant une volonté non équivoque de consentir à cet acte.[10] ». On peut la définir également comme « *le signe par lequel le signataire s'affirme comme l'auteur de ce qu'il signe, marque personnelle intentionnelle qui manifeste son identité et concentre sur sa tête les effets attachés à son initiative*[11] ».

9. **Deux missions** découlent de la signature : identifier son auteur et donc identifier l'auteur de l'acte sur lequel figure la signature, et marquer la volonté de l'auteur d'adhérer à l'acte, *i.e* exprimer son consentement. Ces deux missions permettent de marquer l'engagement des parties. Cependant dans le commerce électronique il est parfois difficile voire impossible de marquer une signature manuscrite. C'est pourquoi l' « électronisation » de la signature était nécessaire. « *La signature électronique, c'est la personne, c'est son consentement ; c'est aussi la plus-value qui s'attache au travail objectif, la justification du prix que l'on paye, la consécration pour le jeune professeur de droit qui prétend à devenir « la » signature dans sa spécialité*.[12] ». Passer d'une écriture à la main à une forme électronique constitue une véritable révolution et un important défi juridique. C'est pour cette raison qu'il faut respecter des conditions techniques sécurisées et garantir l'utilisation d'un système fiable et crédible.

10. La signature « *identifie celui qui l'appose* » et « *manifeste le consentement des parties aux obligations qui découlent de cet acte*[13]».Elle n'est donc pas seulement un moyen d'approuver formellement le contenu de l'acte mais elle participe également à la formation de la relation contractuelle elle-même. Mais comment cette révolution s'est concrètement déroulée dans le système juridique ? A-t-elle connu un succès ?

11. On distingue **deux grandes évolutions en matière de droit de la preuve électronique** et de la **signature électronique** : la Loi du 13 mars 2000[14] transposant la Directive

[10] C. DEVYS, *Du sceau numérique à la signature numérique*, Rapp. OJTI, nov.1995, pub. in OJTI, ss dir. C. DHENIN, *Vers une administration sans papier*, Paris, La documentation française, 1996, p. 96
[11] G. CORNU, Vocabulaire juridique, Coll. PUF, éd. avr. 2007, Paris, p. 866
[12] J. RAYNARD, *Signature électronique, valeur probante, cryptologie et tiers certificateur*, RTD Civ., 2000, p. 449
[13] C. civ., art. 1316-4 al. 1
[14] 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, JO n° 62, 14 mars 2000, p. 3968, t. n° 1 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629200

européenne sur la signature électronique du 13 décembre 1999[15] et la Loi du 21 juin 2004 sur la Confiance en l'Economie numérique[16].

12. Avant la Loi du 13 mars 2000[17], régnait la liberté de la preuve en principe, avec des cas d'exclusion de la preuve électronique.

13. Dans le domaine commercial, **entre professionnels** notamment, la preuve est libre[18]. Cette liberté de preuve a permis alors à l'écrit électronique de se faire sa place sans difficulté. Les moyens de preuve sont soumis à l'appréciation du juge qui peut alors écarter les preuves qui ne respectent pas le principe de loyauté et de proportionnalité.

14. En **droit commun des contrats**, la preuve est libre pour les actes qui ne dépassent pas un certain montant fixé par Décret. En l'occurrence le dernier Décret en la matière met cette somme à 1500 euros[19]. Les actes doivent être passés par écrit. La preuve est également libre en cas de commencement de preuve par écrit[20] ou en cas de circonstances exceptionnelles comme l'impossibilité matérielle ou morale[21].

15. En ce qui concerne les **cas d'exclusion de la preuve électronique**, sont exclus de la preuve électronique les cessions de brevets ou de marques[22] et les contrats de société pour lesquels l'écrit est une condition de validité. Sont également exclues les formalités imposées par certains textes comme le Code de la consommation, et notamment en ce qui concerne les formalités relatives au démarchage. En effet, il existe une obligation de remettre à l'acheteur un formulaire détachable pour l'exercice de son droit de repentir et tous les exemplaires doivent être signés et datés de la main même du client[23].

[15] Dir. 1999/93/CE du Parlement et du Conseil, 13 déc. 1999, sur un cadre communautaire pour les signatures électroniques, JOCE L 13, 19 janv. 2000, p. 12 ;
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:FR:NOT
[16] L. n° 2004-575, 21 juin 2004, pour la confiance en l'économie numérique, dite LCEN, JO 22 juin 2004, p. 11168, t. n° 2, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164
[17] L. n° 2000-230, 13 mars 2000, préc.
[18] C. com., art. L. 100-3
[19] Décr. n° 2004-836, 20 août 2004, JO n° 195, 22 août 2004, p. 15032, t. n° 7
[20] C. civ., art. 1347
[21] C. civ., art. 1348 al. 1
[22] CPI, art. L. 613-8 et L. 714-1
[23] C. conso., art. L. 121-24

16. La Loi du 13 mars 2000[24] donne une reconnaissance juridique à la signature électronique et pose des règles en matière de conflit de preuves. C'est une Loi d'incitation, marquant une avancée significative en matière de signature électronique et surtout de droit relatif à la preuve.

17. La Loi du 13 mars 2000 est issue de travaux d'une commission d'universitaires, remaniée par le Conseil d'Etat. Elle refond les articles 1316 et suivants du Code civil. Deux sortes d'écrits sont donc consacrées : l'écrit en support matériel et l'écrit électronique, avec deux sortes de signatures : manuscrite et électronique. Il est paru nécessaire d'ajouter au réseau Internet des éléments de sécurité complémentaires par la sécurisation apportée par cette Loi, qu'on verra plus tard en ce qui concerne la signature électronique.

18. La même Loi de 2000 a modifié les dispositions du Code civil relatives à la preuve littérale et a admis l'écrit électronique comme mode de preuve. Elle a ainsi su donner une définition juridique de l'écrit qui n'a jamais été consacrée auparavant ; il s'agit 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*[25]. »

19. La consécration juridique de l'écrit a pour corollaire la reconnaissance juridique de la signature électronique. Elle a été consacrée par la Directive européenne sur la signature électronique du 13 décembre 1999[26] transposée en France par la Loi du 13 mars 2000 et son Décret d'application du 30 mars 2001[27], Décret du 18 avril 2002[28] et l'Arrêté du 31 mai 2002[29].

20. La **CNUDCI[30]** avait en 1996 proposé une Loi-type sur le commerce électronique[31], visant à harmoniser les législations entre les Etats membres des Nations Unies. C'est pourquoi

[24] L. n° 2000-230, 13 mars 2000, préc.
[25] C. civ., art. 1316
[26] Dir. 1999/93/CE, 13 déc. 1999, préc.
[27] Décr. 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, p. 5070 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796
[28] Décr. n° 2002-535, 18 avr. 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 avr. 2002, p. 6944 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005632663
[29] Arr. 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 2002, p. 10223 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023888760
[30] Commission des Nations Unies pour le Droit Commercial International

la Commission européenne en 1998 a fait une proposition sur le commerce électronique[32] au Parlement européen. Après quelques amendements et modifications, une position commune est née le 4 mai 2000[33], menant à l'adoption de la Directive le 8 juin 2000[34] « *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* » dite Directive « *sur le commerce électronique* ».L'objectif de cette Directive est d'établir des règles assurant la « libre circulation des services de la société d'information entre les Etats membres ». Ce texte constitue une avancée majeure dans le domaine du commerce électronique, berceau de l'utilisation de l'écrit électronique et de la signature électronique.

21. Le développement du commerce électronique pousse à la réflexion. La Loi du 13 mars 2000 est importante pour deux raisons :

-elle marque l'entrée officielle du commerce électronique dans le Code civil ;
-elle donne une définition de l'écrit et de la signature électronique.

22. La Loi de 2000[35] s'inscrit dans une stratégie globale d' « *entrée dans la société de l'information*[36] ». « *La Loi du 13 mars 2000 a créé un embryon de cycle de vie pour l'écrit sous forme électronique : il est d'abord établi (art. 1316-1), puis transmis (art. 1316) et enfin conservé (art. 1316-1) lorsque les effets juridiques qui en découlent sont définitivement protégés*[37]. »

23. Après la Loi du 13 mars 2000[38], apparait la Loi du 21 juin 2004 dite LCEN[39] complétée par l'Ordonnance du 16 juin 2005[40]. Ces deux textes ont un impact important, ils achèvent l'avènement de la construction légale et réglementaire.

[31] L. type CNUDCI, 16 déc. 1996, sur le commerce électronique, A/RES/51/162 ; www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf
[32] Proposition transmise au Parlement européen le 23 déc. 1998, JOCE n° C 30, 5 fév. 1999, p. 4
[33] Position commune 28 fév. 2000, CE n° 22/2000, JOCE n° L. 128, 8 mai 2000, p. 32 et s.; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000AG0022:FR:NOT
[34] Dir. 1999/93/CE, 13 déc. 1999, préc.
[35] L. n° 2000-230, 13 mars 2000, préc
[36] Terme communautaire désignant l'Internet
[37] T. PIETTE-COUDOL, *LCEN. L'écrit électronique et la signature électronique depuis la LCEN*, CCE, n° 9, 9 sept. 2004, Etude 29, p. 3,
[38] L. n° 2000-230, 13 mars 2000, préc.
[39] L. n° 2004-575, 21 juin 2004, préc.

24. Les écrits exigés pour la validité d'un acte juridique peuvent être sous forme électronique[41] depuis la Loi du 21 juin 2004 dite LCEN[42]. Les conditions de validité d'un écrit sous forme électronique n'ont pas été décrites dans la Loi de 2000[43]. La Loi de 2004 est donc intervenue dans cette matière. De plus, l'Ordonnance du 16 juin 2005[44] complète la Loi du 21 juin 2004 dans le Code civil quant à la **validité du contrat électronique**. Elle permet ainsi l'accomplissement de certaines formalités pour la conclusion, la validité ou les effets de certains contrats[45]. Par exemple, il est précisé dans ce texte que les informations requises pour la conclusion du contrat peuvent être transmises par *email* si le destinataire l'accepte, sachant que le professionnel ne peut pas refuser ce moyen de communication.

25. Aussi, la signature électronique est suivie souvent d'un **dispositif de sécurisation** que permet le certificat électronique, via un composant technique spécifique pour lequel les prestataires de service de certification électronique peuvent voir leur responsabilité professionnelle engagée dont les modalités n'étaient pas précisées par notre droit.

26. La Loi de 2004 comble également un vide juridique qui existait sous la Loi de 2000. La doctrine pensait que l'écrit *ad probationem* était consacré, mais pas l'écrit *ad validitatem*. La Loi de 2004 comble ce manque en créant l'**article 1108-1 du Code civil** qui dispose qu'un écrit peut être établi et conservé sous forme électronique lorsqu'un écrit est exigé pour la validité de l'acte.

27. Enfin, la Loi de 2004 reprend un principe posé par la Directive du 8 juin 2000[46] dite « *Commerce électronique* » qui a prescrit la **dématérialisation des contrats électroniques**. La Loi de 2004 a transposé ce principe en insérant dans le Code civil les articles 1369-1 à 1369-3.

---

[40] Ord. n° 2005-674, 15 juin 2005, relative à l'accomplissement de certaines formalités contractuelles par voie électronique, JO 17 juin 2005 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000448268

[41] C. civ., art. 1108-1

[42] L. n° 2004-575, 21 juin 2004, préc.

[43] L. n° 2000-230, 13 mars 2000, préc.

[44] Ord. n° 2005-674, 15 juin 2005, préc.

[45] C. civ., art. 1369-1 et s.

[46] Dir. n° 2000/31/CE, 8 juin 2000, « Commerce électronique », JO n° L 178, 17 juill. 2000, p. 0001-0016 ; http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FR&numdoc=32000L0031&model=guichett

28. Plusieurs questions se posent. Quelles sont les **conséquences juridiques** du développement de l'écrit électronique et surtout de la signature électronique ? Mais avant tout, quel est son mécanisme ? Comment a-t-elle su se faire une place dans le droit, et a-t-elle connu un succès ? Est-elle une source de sécurité ? Quels sont ses atouts, ses éventuelles lacunes ? L'écrit électronique et son corollaire qu'est la signature électronique ont su bouleverser le système juridique. Mais la problématique se situe surtout au niveau de la **sécurité** qu'elle apporte. L'**efficacité** d'un tel mécanisme suffit-elle ? Comment peut-elle assurer une sécurité aux utilisateurs et ses destinataires ? Est-elle réellement fiable ? Une signature simple et non sécurisée peut-elle apporter autant de fiabilité qu'une signature sécurisée ? Quelle est donc leur différence et leur conséquence juridique ? Enfin, dans quels domaines se développe-t-elle, comment, quel est l'ampleur de ce développement ?

29. L'avènement progressif de la signature électronique apporte des effets juridiques révolutionnaires. La signature électronique couvre désormais un domaine dont l'importance s'explique par le double intérêt qu'elle présente : l'efficacité (PARTIE I) et la sécurisation (PARTIE II).

PARTIE I. L'EFFICACITE DE LA SIGNATURE ELECTRONIQUE

30. *La signature électronique relève d'un mécanisme efficace (Chapitre I). Au-delà de cette efficacité intrinsèque, elle est également un moyen de preuve (Chapitre II).*

Chapitre I : L'efficacité du mécanisme de la signature électronique

31. La signature a deux rôles primordiaux: l'identification et l'engagement de son auteur. Pour que la réussite de cette mission par la signature électronique se fasse autant que la signature manuscrite, elle se doit d'avoir un mécanisme efficace. Deux questions se posent alors : Comment fonctionne la signature électronique ? (Section 1) La signature simple est-elle également efficace ? (Section 2).

Section 1 : Le fonctionnement de la signature électronique

32. « *La signature électronique consiste en l'usage d'un processus fiable et garantissant le lien avec l'acte sur lequel elle porte*[47]*.* » *La signature électronique utilise la technique de la cryptographie (§1) pour que le processus se mette en place (§2).*

[47] C. civ., art. 1322-1

§ 1 La technique de la cryptographie

33. Le **mécanisme** de la signature électronique repose sur la technique de la « cryptographie asymétrique », qu'on appelle aussi « cryptographie à double clef » ou « cryptographie à clef publique », qui a pour origine la science de la cryptologie.

34. Mais qu'est-ce que la **cryptologie** ? La cryptologie est appelée communément la « science du secret ». C'est un art ancien (Jules César l'utilisait) mais elle est devenue une source de recherche scientifique à partir de 1970. Il s'agit d'un « *ensemble de moyens, tant logiciels que matériels, pour rendre une information inintelligible, puis pour la restituer dans son état premier*[48]. ».

35. La technique de la cryptographie se divise en deux sortes:

-la cryptographie à clef secrète, appelée aussi symétrique ou bien classique ;
-la cryptographie à clef publique, appelée également asymétrique ou moderne.

36. La première clef est la plus ancienne puisqu'elle remonte à l'Égypte de l'an 2000 avant J-C. La seconde remonte à 1976. Les clefs sont alors différentes et ne peuvent se déduire l'une de l'autre. Ils rendent les messages incompréhensibles. La cryptologie a très longtemps été considérée comme une **arme de guerre**. On peut citer en exemple la Première Guerre mondiale. En effet, le « Room 40 » était un service de chiffrement britannique. Il a décrypté un télégramme envoyé en 1917 de Berlin à l'ambassadeur allemand à Washington, qui devait le retransmettre au Mexique. Les américains ont pu apprendre que l'Allemagne allait enclencher une guerre sous-marine et qu'elle demandait une alliance militaire, pour que le Mexique puisse récupérer le Nouveau-Mexique, le Texas et l'Arizona.

37. Puis l'usage de la cryptographie est devenu libre dans un contexte de **développement de l'informatique et des télécoms**, avec la Loi du 29 décembre 1990[49] sur la réglementation

[48] T. PIETTE-COUDOL, *Echanges électroniques, Certification et sécurité*, Coll. Maitriser, éd. Litec, Paris 2000, p. 15, §25
[49] L. n° 90-1170, 29 déc. 1990, sur la réglementation des télécommunications, JO n°303, 30 déc. 1990, p. 16439; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006076972

des télécommunications, qui a été réformée en 1996[50], puis réaménagée par un Décret en 1999[51]. Les **fournisseurs** sont assujettis à des formalités et notamment le dépôt en deux exemplaires de matériels ou logiciels mettant en œuvre les prestations cryptographiques, et notamment en ce qui concerne la signature électronique :

-protection du mot de passe, des codes d'identification ou données d'authentification ;
-élaboration et protection d'une procédure de signature ;
-vérification de la source de données ;
-preuve de la remise des données au destinataire ;
-détection des altérations du support risquant de porter atteinte aux données.

38. L'usage de la cryptographie est puni lorsqu'il a pour objet de préparer ou de commettre un crime ou un délit, ou encore pour en faciliter la préparation ou la commission[52].

39. Grâce à un logiciel spécifique, un résumé du message est calculé à partir d'un **algorithme de hachage**, *i.e* des algorithmes mathématiques. Un ensemble de produits cryptographiques utilisent une clef privée pour verrouiller (chiffrer) le message avant l'émission et une clef publique pour déverrouiller le message chiffré arrivé. Le résumé est chiffré avec la clef privée de l'utilisateur et le destinataire reçoit le résumé. Ce dernier le déchiffre avec la clef publique. C'est ce mécanisme de hachage qui permet de vérifier la signature. Cette méthode sécurise les échanges de données et les transmissions de données, appelée « chiffrement ». Ainsi, un signataire détient deux clefs grâce à son logiciel de messagerie électronique. Il s'agit d'une clef « privée » que seul le signataire connait, et d'une clef « publique » qui est alors connue du destinataire. A chaque clef publique correspond une clef privée et inversement. Ces deux bi-clefs sont appliquées pour la signature électronique mais pas uniquement. On les retrouve également pour le paiement sécurisé des échanges commerciaux électroniques. En effet le paiement doit éviter toute fraude. Il utilise des moyens cryptographiques spécifiques, qui se partagent avec la signature électronique.

[50] L. n° 96-659, 26 juill. 1996, de réglementation des télécommunications, JO n° 174, 27 juill. 1996, p. 11384 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000733177
[51] Décr. n° 99-200, 17 mars 1999, définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable, JO n° 66, 19 mars 1999, p. 4051; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005627660
[52] C. pen., art. 132-79

40. Se pose maintenant la question de savoir quel est le processus de la signature électronique.

§ 2 Le processus de la signature électronique

41. La signature électronique doit respecter un **processus** précis, à savoir :

-le signataire signe son message électronique avec sa clef privée ;
-le destinataire vérifie l'authenticité de la signature en utilisant la clef publique du signataire (si le signataire n'avait pas auparavant transmis sa clef publique au destinataire, ce dernier peut dans ce cas consulter directement un annuaire spécialisé qui est consultable sur Internet) ;
-le destinataire doit être sûr que la clef publique qu'il a reçue est bien celle qui émane du signataire. Cette vérification se fait au moment même de l'authentification. La clef publique ne doit pas être frauduleuse ou bien révoquée par le signataire. C'est le certificat électronique qui jouera le rôle d'intermédiaire entre les deux[53]. La signature électronique est nominative et ne vise que le signataire. Elle n'assure pas de protection particulière des données qui sont transmises au destinataire. S'il veut sécuriser son document, il doit donc le chiffrer en utilisant une clef privée et publique comme pour la signature électronique.

42. Les signatures électroniques sont un bon moyen de **garantie** et d'**authenticité** en ce sens qu'elles assurent l'origine des informations et contrôlent l'absence de fraude grâce à la carte à puce et la carte de mémoire. C'est ce qui les différencie de la signature manuscrite : elle n'a que le rôle d'identification de l'auteur mais n'assure pas l'intégrité du message ni d'en assurer le secret. Ces fonctions sont les plus importantes de la signature électronique.« *On peut s'interroger sur la formule 'Je crypte donc je suis !' ; peut-on y voir l'amorce d'un nouveau courant de pensée pour le siècle prochain* ?[54] » cite un auteur. En effet, l'émergence et le succès de l'écrit électronique, de l'informatique et des relations contractuelles électroniques dans un sens général devient une véritable philosophie, où la présence humaine n'est plus obligatoire, où les relations contractuelles électroniques sont

[53] Cf. infra, PARTIE II, Chapitre I, Section 2, II, B.
[54] E. A CAPRIOLI, *Sécurité et confiance dans le commerce électronique : signature numérique et autorité de certification*, JCP G., n° 14, 1er avr. 1998, I 123, p. 2, §6

rapides, efficaces et sécurisées : on assiste à une déshumanisation, une dépersonnalisation des échanges.

43. La Directive européenne du 13 décembre 1999[55] consacre deux types de signature électronique : la signature « ordinaire » et la signature « avancée ». La signature « ordinaire » est « *une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et sert de méthode d'authentification*[56] ». La signature électronique « avancée » ou sécurisée est une signature électronique qui satisfait à des exigences cumulatives qu'on verra dans la seconde partie.

44. Quelle est concrètement l'efficacité d'une signature électronique simple et quel exemple peut-on apporter ?

Section 2 : La signature électronique « simple »

45. La signature numérique peut être assimilée à la signature électronique simple puisqu'elle répond aux exigences légales (§1) contrairement à la signature numérisée (§2).

§ 1 La signature numérique

46. La **signature** numérique ou générique s'inscrit dans un cadre plus général que celui de la signature électronique. Elle est définie par la norme ISO 7498-2[57] relative à l'architecture de sécurité pour les systèmes ouverts comme des « *données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données permettant à un destinataire de*

[55] Dir. 1999/93/CE, 13 déc. 1999, préc.
[56] Dir. 1999/93/CE, 13 déc. 1999, préc., art. 2.1
[57] « *International Organization for Standardisation* », « *Document établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats garantissant un niveau d'ordre optimal dans un contexte donné*. » ; *Directives ISO/CEI*, part. 2, « Règles de structure et de rédaction des Normes internationales », 5ème éd., 2004, §3.1

prouver la source et l'intégrité de cette unité en la protégeant contre la contrefaçon. ». Cette définition est très proche de celle de la signature électronique…

47. Selon la **CNUDCI**, « *Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données : a) Si une méthode est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données ; et b) Si la fiabilité ce cette méthode est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière* (…) [58]»La CNUDCI est venue également donner une **définition de la signature numérique**. Selon elle, la signature numérique est « *une valeur numérique apposée à un message de données et qui, grâce à une procédure mathématique bien connue associée à une clef cryptographique privée de l'expéditeur, permet de déterminer que cette valeur numérique a été créée à partir de la clef cryptographique privée de l'expéditeur. Les procédures mathématiques utilisées pour créer les signatures numériques sont basées sur le chiffrement de la clef publique. Appliquées à un message de données, ces procédures mathématiques opèrent une transformation du message de telle sorte qu'une personne disposant du message initial et de la clef publique de l'expéditeur peut déterminer avec exactitude : a) si la transformation a été opérée à l'aide de la clef privée correspondant à celle de l'expéditeur ; et b) si le message initial a été altéré une fois la transformation opérée (…)*[59] »

48. La signature numérique sert à **authentifier** un message électronique. L'émetteur du message peut être identifié et authentifié au moyen de la clef publique correspondant à sa clef privée. Quant au **processus de signature numérique**, il se déroule ainsi :

-création d'une paire de clefs propres à l'utilisateur ;
-rédaction d'un message sur l'ordinateur ;
-préparation d'un abrégé du message par l'expéditeur ;
-chiffrement de l'abrégé par l'expéditeur avec sa clef privée ;
-adjonction de la signature numérique au message par l'expéditeur ;

[58] Rapp. Comm. Nations Unies pour le droit commercial international sur les travaux de sa vingt-neuvième session, 28 mai-14 juin 1996, Assemblée générale, Documents officiels, Cinquante et unième session, suppl. n° 17 (A/51/17), V. p. 77

[59] CNUDCI, note du Secrétariat, Doc. A/CN.9/WG.IV/WP.71, 31 déc. 1996, V. § 55.V. également CNUDCI, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente et unième session, Doc. A/CN.9/437, 12 mars 1997

-l'expéditeur envoie le message signé par le réseau ;
-le destinataire utilise la clef publique de l'expéditeur pour vérifier la signature numérique de l'expéditeur ;
-le destinataire créé un abrégé du message avec le même algorithme que l'expéditeur ;
-le destinataire compare les deux abrégés afin de vérifier l'intégrité du message ;
-le tiers certificateur délivre un certificat au destinataire qui confirme que la signature numérique du message est bien celle de l'expéditeur. Il a pour mission d'administrer le système de signature numérique.[60]

49. La signature générique peut-elle donc suffire ? Est-elle suffisamment sécurisée ? Jusqu'à présent aucune réponse claire n'est apportée par la doctrine. C'est pourtant dans la pratique la signature la plus utilisée par les consommateurs. Elle est une signature électronique simple, non sécurisée, mais non pas sans effet juridique. Elle prouve l'identité de l'auteur de l'acte donc elle est un moyen de preuve comme la signature électronique (et comme la signature manuscrite). Elle assure l'intégrité de l'acte également, c'est-à-dire qu'elle assure que l'acte n'a pas été modifié ou altéré ; et protège de la contrefaçon, elle est donc efficace et fiable. Seulement, la différence jouera lors d'un contentieux. La fiabilité d'une telle signature ne sera pas présumée, ce qui jouera sur la charge de la preuve[61]…On parle de « signature numérique » plutôt que signature « électronique » dans un moyen technico-informatique, en dehors de toute référence juridique. La signature électronique quant à elle fait référence aux conséquences juridiques qu'elle engendre, notamment lorsqu'elle est sécurisée.

50. « *La signature numérique, si elle porte en clair le nom du contractant, n'offre aucune sécurité aux parties, car quiconque peut usurper le nom d'autrui à des fins malhonnêtes*[62]. » pense Pierre Catala. La signature électronique non sécurisée ou bien « simple », n'est donc pas sans effet juridique, mais les effets juridiques sont différents comme on le verra ultérieurement.

51. La signature numérisée est également bien différente de la signature électronique :

[60] CNUDCI, note du secrétariat, Doc. A/CN.9/WG.IV/WP.71, 31 déc. 1996, préc., V. § 45
[61] Cf. infra, PARTIE II, Chapitre II, Section 2, II
[62] P. CATALA, *L'introduction de la preuve électronique dans le code civil*, JCP G. n° 47, 24 nov. 1999, I 182, p. 4, §8

§ 2 La signature numérisée

52. On l'appelle aussi **signature** « **scannérisée** » ou encore « digital signature » en anglais. A la différence de la signature électronique elle assure la sécurité technique du message en assurant l'intégrité et l'identification, alors que la signature électronique en assure la sécurité juridique. On peut citer un arrêt en exemple pour marquer la différence entre une signature électronique et une signature numérisée, il s'agit du premier arrêt sur la signature électronique. Dans un arrêt rendu par la Cour d'appel du 20 octobre 2000[63], les moyens utilisés par l'avocat pour réaliser son acte de procédure ont été mis en cause. L'avocat de la SARL avait en effet utilisé une signature scannérisée sur la déclaration d'appel[64]. Dans cet arrêt, la Cour d'appel rejette la signature scannérisée comme moyen de preuve d'identité de la signature et de fiabilité, ce qui nous pousse à conclure que le seul moyen sécurisé est la signature électronique ou numérique. Elle précise : « *En conséquence, les dispositions de ce texte sont inapplicables en l'espèce d'autant plus que le décret destiné à préciser les conditions de la fiabilité d'identification de la personne qui appose la signature n'est pas encore paru à la date des débats devant la cour. Partant, la cour n'est pas en mesure d'apprécier le degré de fiabilité du processus décrit par l'appelante au regard d'un texte dont la parution est attendue. La fiabilité du procédé utilisé en l'espèce par l'avocat est au demeurant toute relative dans la mesure où le code permettant d'accéder à la signature peut être détenu par une autre personne du cabinet. L'identification de la personne ayant recours à la signature informatique est dès lors très incertaine.* ».

53. Conformément à l'article 5 de la Directive de 1999[65], la signature électronique et la signature manuscrite ont une **valeur équivalente**. En vertu du **principe de non-discrimination**, les effets juridiques de la signature ne peuvent pas être écartés au motif qu'elle n'a pas été certifiée par un prestataire de services accrédité. Cela signifie que l'équivalence de la signature électronique et de la signature manuscrite instaure une **présomption de fiabilité**.

[63] CA Besançon, Ch. soc., 20 oct. 2000, SARL Chalets Boisson c/ Gros, JCP G. 2001, II, n° 10606, note E. A Caprioli
[64] Un jugement rendu par le Conseil de prud'hommes avait condamné à des dommages et intérêts une SARL pour licenciement abusif d'un salarié. La SARL interjette appel.
[65] Dir. 1999/93/CE, 13 déc. 1999, préc.

54. Ainsi dans l'arrêt d'appel il s'agit d'une signature scannérisée et non électronique ; elle ne rentre donc pas dans la présomption de fiabilité prévue par la Directive. La signature scannérisée est bien différente de la signature électronique : elle repose sur la **numérisation** d'une signature qui peut être enregistrée dans la mémoire d'un ordinateur ou peut être copiée dans un autre fichier et ensuite imprimée. Le document obtenu ne peut donc avoir la même force probante qu'un document original papier, sauf si les parties l'avaient prévu dans une convention. La Cour rappelle la fonction de la signature électronique : **identifier** le signataire. Or, la signature scannérisée ne garantit pas le lien entre la signature et le signataire puisqu'elle peut avoir été faite par n'importe qui… L'arrêt relève que « *la fiabilité de ce procédé (…) est au demeurant toute relative* ».

55. Le Décret de 2001[66] rappelle les conséquences divergentes au niveau de la preuve. La fiabilité du procédé de la signature électronique est présumée jusqu'à la preuve du contraire, lorsque ce procédé met en œuvre une signature électronique sécurisée dont la vérification repose sur l'utilisation d'un certificat électronique qualifié. Il en résulte deux conséquences :

-en cas de contestation sur la signature électronique, et qu'elle réponde aux conditions fixées par le Décret, la preuve appartient à celui qui conteste la fiabilité de celle-ci ;
-si la signature électronique n'a pas été certifiée par un prestataire de services de certification électronique, la charge de la preuve se trouve renversée, c'est la personne qui déclare la fiabilité de la signature qui doit en rapporter la preuve. En l'espèce, la signature est scannérisée, elle ne rentre pas dans la première conséquence de la disposition apportée par le Décret donc c'était à la SARL de prouver la fiabilité de cette signature. La signature numérisée ne peut alors être considérée que comme un commencement de preuve plutôt qu'une véritable preuve écrite.

56. *On pourrait conclure ainsi que la signature scannérisée n'apporte donc pas autant d'efficacité que la signature électronique tandis que la signature électronique est un outil efficace d'identification et d'intégrité de l'acte sur lequel elle est apposée. Mais comment prouver avec un écrit électronique, une signature électronique et non manuscrite ? Quel est le changement juridique de la consécration de cet outil ?*

[66] Décr. n° 2001-272, 30 mars 2001, préc.

Chapitre II : La signature électronique comme moyen de preuve

57. La consécration de la signature électronique est passée par la reconnaissance juridique de l'équivalence entre l'écrit papier et électronique (Section 1) et par la possibilité de mettre en cause la responsabilité des prestataires de services de certification électronique (PSCE) (Section 2).

Section 1 : L'équivalence entre l'écrit papier et l'écrit électronique

58. L'apparition légale de la définition de l'écrit (§1) et l'adaptation des règles de l'écrit (§2), marquent la reconnaissance de l'équivalence entre l'écrit électronique et l'écrit papier.

§ 1 L'attribution d'une définition légale à l'écrit

59. Le droit français distingue la preuve des actes juridiques de la preuve des faits juridiques. Si la preuve des faits juridiques est libre, ce n'est pas le cas des actes juridiques. L'**acte juridique** tout d'abord est « *une opération juridique consistant en une manifestation de volonté ayant pour objet et pour effet de produire une conséquence juridique*[67] ».En principe, le droit français n'est soumis à aucun formalisme pour qu'un acte soit valable. C'est l'autonomie de la volonté qui prime. Le consensualisme découle du principe d'autonomie de la volonté. Un contrat entre des parties naît du seul échange du consentement. Puis, ce n'est que par exception que le droit impose un certain formalisme à respecter par les parties, auquel

[67] G. Cornu, *Vocabulaire juridique*, Association H. Capitant, éd. PUF, Paris, avr. 2007, p. 17

cas contraire l'acte n'est pas valable. Le **fait juridique** est à l'inverse tout « fait quelconque auquel la loi attache une conséquence juridique qui n'a pas été nécessairement recherchée par l'auteur du fait ». La preuve des faits juridiques est libre.

60. Dès 1804, le Code civil a prévu des **règles simples liées à la preuve** en droit des obligations Domat définissait la preuve littérale comme « *la force des preuves par écrit (qui) consiste en ce que les hommes sont convenus de conserver par l'écriture le souvenir des choses qui se sont passées et dont ils ont voulu faire subsister la mémoire, pour s'en faire des règles, ou avoir une preuve perpétuelle de la vérité de ce qu'on écrit*.[68] ». Puis se sont développés les contrats de consommation, liés au développement de la consommation, des services, des contrats spéciaux comme la vente, le bail, le crédit, les assurances… L'exigence d'un écrit a donc pris de l'ampleur. A la fin du XXème siècle, a eu lieu une évolution technologique qui a créé de nouveaux modes de communication électronique entre les hommes comme la télécopie, la transmission numérique…Le commerce électronique se développe de plus en plus, les contrats se font par des moyens autres que par écrit : c'est le cas des échanges électroniques au moyen d'*email*. Selon P-Y Gautier, le papier ne va pas disparaitre, ce sont au contraire « *deux modes alternatifs contractuels qui vont se mettre en place. Il n'y a pas de « tout internet », gardons la tête froide s'il vous plait.*[69] »

61. Des textes sont donc apparus pour adapter le droit aux nouvelles technologies comme nous l'avons vu précédemment, puis l'écrit a enfin reçu une **définition légale**. Pourquoi si tardivement ? Parce que l'écrit s'identifiait par principe à tout accord de volontés par écrit. Cette logique était surtout valable en droit des obligations, car dans les autres domaines l'écrit n'était pas forcément pris dans un sens strict. En effet l'accord de volontés, surtout pour le testament olographe, pouvait être inscrit sur un mur, une glace, un petit bout de tissu, et pouvait l'être avec un autre moyen qu'un stylo (couteau, charbon, sang…).

62. En ce qui concerne la Directive de 1999[70], son article 9 prévoit que « *Les Etats membres veillent à ce que leur système juridique rende possible les contrats par voie électronique. (…) Ils s'assurent notamment que le régime applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ou ne conduise à priver d'effet et de validité*

[68] Domat, *Les lois civiles*, I, III, VI, II
[69] P-Y GAUTIER, *Le bouleversement du droit de la preuve : vers un mode alternatif de conclusion des conventions*, PA n° 26, 7 févr. 2000, p. 4, §3
[70] Dir. 1999/93/CE, 13 déc. 1999, préc., art. 6.1 et 2

de tels contrats, pour le motif qu'ils sont passés par voie électronique. ». Or en France il y a certains contrats qui sont soumis à la solennité *ad validitatem*, qui pourrait être perçue comme un obstacle à l'usage du numérique… Cependant la **Jurisprudence** a eu son rôle à jouer, elle a montré sa faculté d'adaptation aux évolutions techniques et de reproduction et de communication à distance, notamment en ce qui concerne la force probante des documents électroniques.

63. On peut citer à titre d'exemple deux arrêts rendus par la Cour de cassation. Le premier est un arrêt rendu en 1992[71] : la Haute Cour a reconnu la portée juridique d'une photocopie, en tant que commencement de preuve par écrit. On voit bien que la Jurisprudence met toute l'importance sur l'authenticité et l'intégrité du message, c'est le cas dans l'arrêt célèbre sur le Bordereau Dailly de 1997[72]. Ce qui compte c'est l'**expression de la volonté**, pas forcément le moyen d'expression. Pour illustration, P-Y Gautier précise : « *Identité, fiabilité, intégrité, telle est la trilogie de nature à s'assurer que le message émane bien de celui auquel on l'impute.*[73]». Ensuite, le deuxième arrêt est un arrêt célèbre rendu par la Chambre commerciale en date du 2 décembre 1997[74]. La Haute Cour a énoncé les conditions nécessaires à la valeur probatoire d'un document produit par télétraitement, à propos d'une créance Dailly : « *Mais attendu que l'écrit constituant, aux termes de l'article 6 de la loi du 2 janvier 1981, l'acte d'acceptation de la cession ou du nantissement d'une créance professionnelle peut être établi et conservé sur tout support, y compris par télécopies, dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées*. »

64. Ainsi, la **banalisation d'Internet et le développement du télé-contrat** envahissent la vie quotidienne et le monde des affaires, en devenant un phénomène de masse, le télé-contrat échappe au droit des affaires et se « civilise » au sens juridique. A la suite de ce phénomène, le Ministère de la Justice a chargé le Groupe « Droit et Justice[75] » de constituer un groupe d'universitaires pour une étude approfondie de ce thème. Un avant-projet de loi est sorti en 1998, relatif à l'adaptation du droit de la preuve aux nouvelles technologies, pour répondre aux demandes législatives dues à la mesure du phénomène. L'informatique n'est plus réservé

[71] Cass. com., 15 déc. 1992, Bull. civ. IV, n° 419
[72] Cass. com., 2 déc. 1997, préc.
[73] P-Y GAUTIER, *Le bouleversement du droit de la preuve : vers un mode alternatif de conclusion des conventions*, PA n° 26, 7 févr. 2000, p. 4, §8
[74] Cass. com., 2 déc. 1997, JCP G. 1998, II, 10097, note Grynbaum; JCP E. 1998, n°5, p. 178, note T. Bonneau
[75] Cf. http://www.droitetjustice.org/article.php?id=3

aux avertis, mais il est devenu le moyen de communication ordinaire de professionnels ou de simples particuliers. Le temps était alors venu de reconnaître que les messages électroniques peuvent laisser des preuves des transactions auxquelles elles ont abouti.

65. La **définition de l'article 1316 du Code civil,** apportée par la Loi de 2000,[76] introduit deux éléments : l'écrit est d'abord défini. Il s'agit d'une séquence de lettres, de signes, de chiffres ou autres symboles, qui doivent être ordonnés de manière intelligible pour le destinataire. Ensuite, l'article 1316-1 du Code civil élève la preuve électronique au même rang que les preuves littérales si deux conditions sont respectées : que soit identifié celui dont il émane et que les conditions dans lesquelles il a été établi et conservé en garantissent sa fiabilité. A titre d'exemple, on peut citer un arrêt rendu par la Première Chambre civile de la Cour de cassation le 13 mars 2008[77] : la Cour retient qu'un créancier peut se prévaloir d'un acte sous seing privé dactylographié pour obtenir le remboursement de sa dette. Il s'agissait d'un acte électronique signé de manière numérique. La Jurisprudence l'a accepté au même titre qu'un écrit papier puisqu'il répondait aux exigences du Code civil.

66. L'émergence d'une définition de l'écrit et l'élévation de l'écrit électronique au même rang que l'écrit support papier n'est pas le seul changement. Les règles appliquées habituellement à l'écrit papier doivent être adaptées à l'écrit électronique.

§ 2 L'adaptation des règles contractuelles à l'écrit électronique

67. « *En amont de la problématique de la preuve électronique, l'article 1108 du Code civil constitue une autorisation générale de dématérialiser. (...) Il est permis de procéder à la dématérialisation d'un acte juridique dans la mesure où l'objet en résultant est susceptible de constituer une preuve*[78]. ».

68. L'émergence de l'écrit électronique nécessite l'adaptation des règles de forme (A) et des règles de preuve (B) de l'écrit support papier.

[76] L. n° 2000-230, 13 mars 2000, préc.
[77] Civ. 1ère, 13 mars 2008, n°06-17.534, Bull. civ. I, n°73
[78] T. PIETTE-COUDOL, *La remise électronique du bulletin de paie*, JCP S. n° 43, 26 oct. 2010, 1140, p. 2

A. L'adaptation des règles de forme au contrat commercial

69. Puisque les deux formes d'écrit sont mises au même rang, électronique et papier, le formalisme et les règles de preuve sont les mêmes. C'est ainsi que le **formalisme documentaire** doit être respecté dans les deux cas d'écrit. Il s'agit des règles de forme ainsi que les formalités nécessaires à la formation d'un acte. A l'occasion de l'adoption de la « *Loi modèle pour le commerce électronique*[79] », la CNUDCI a développé la **théorie de « l'équivalent fonctionnel »**. Il s'agit de trouver un équivalent d'une règle de formalisme propre à un écrit support papier à un écrit électronique. Quand il s'agit de formalisme documentaire on pense aux trois éléments significatifs : le support, la signature et les mentions obligatoires. Dans ces cas où la validité d'un acte est subordonnée à des formalités, un équivalent est trouvé en électronique en deux temps : le juriste qui sera confronté à ce genre de situation devra dans un premier temps dématérialiser le document, et dans un second temps il le revalidera dans sa forme juridique électronique.

70. Les mentions obligatoires sont traitées à l'article 1108-1 du Code civil. Les mentions obligatoires présentes sur l'écrit support papier doivent être présentes sur l'écrit électronique : c'est le parallélisme des formes. Il précise : « *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*[80]. ».Dans le domaine de l'**offre contractuelle commerciale électronique**, l'article 1369-3 alinéa 1 du Code civil précise que « *Quiconque propose la fourniture de biens ou la prestation de services par voie électronique indique, de manière claire et compréhensible, les éléments essentiels du contrat proposé, notamment les conditions générales et les tarifs applicables ainsi que les moyens de les conserver et de les reproduire*. ». Il s'agit ici des **situations relationnelles électroniques non professionnelles**, en dehors de toute activité professionnelle et en dehors de toute sollicitation commerciale préalable. On voit bien que les règles applicables à l'écrit support papier dans le cadre d'un échange commercial sont applicables à l'écrit électronique. C'est uniquement le support qui change. Cependant pour les **offres faites par un professionnel**, l'article 1369-1 alinéa 1 et alinéa 2 du Code civil s'appliquent. Le dernier article impose des conditions d'offre plus strictes à respecter pour une relation électronique, dans le cadre d'une activité professionnelle.

[79] Cf. www.uncitral.org
[80] C. civ., art. 1108-1

71. Les **entreprises offrantes** doivent indiquer certaines mentions :

-les étapes à suivre pour négocier et conclure ;
-le moyen de corriger les erreurs ;
-les langues proposées pour la conclusion du contrat ;
-les modalités d'archivage du contrat et les conditions d'accès ;
-les conditions d'accès électronique aux éventuels codes déontologiques de l'offrant.

72. Pour ce qui est de la **conclusion du contrat**, l'article 1369-4 du Code civil dispose que « *Le contrat proposé par voie électronique est conclu quand le destinataire de l'offre ayant passé une commande dont le professionnel a accusé réception confirme son acceptation des conditions de l'offre.* ». On ne peut oublier les deux théories qui gouvernent le droit français sur l'acceptation : l'émission et la réception. La Jurisprudence française a tendance à préférer la théorie de l'émission lorsque la législation ne pose pas de règles spécifiques et protectrices du consommateur (la Directive du 8 juillet 2000 sur le Commerce électronique[81]quant à elle semble préférer la théorie de la réception car elle oblige l'offrant à en informer l'acceptant).

73. Dans le cadre d'un **contrat commercial électronique**, la procédure est ainsi :

-l'offre reçue par le destinataire est acceptée ;
-l'offrant reçoit cette acceptation ;
-l'acceptant reçoit à son tour la réitération des conditions de vente et l'accusé réception de son acceptation.

Ici l'offre est renouvelée mais le contrat n'est pas encore formé : l'auteur de la commande doit réitérer son acceptation : c'est la **pratique du « double-clic »** qui consiste à interroger deux fois le contractant pour être sûr qu'il a bien lu et compris. C'est le second clic qui marque la conclusion du contrat. Le premier clic consiste à vérifier que le contractant est consentant, et le second clic consiste à vérifier que le premier clic est bien certain. C'est biensûr le double clic qui constitue le consentement du contractant. Il est associé à la

[81] Directive 2000/31/CE du Parlement européen et du Conseil, 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»), JO n° L 178, 17 juill. 2000, p. 0001-0016 ; http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FR&numdoc=32000L0031&model=guichett

procédure d'authentification, de non-répudiation et de protection de l'intégrité des messages. Le double-clic constitue donc une signature électronique simple !

74. Pour conclure sur ce point, notons que le Décret du 2 février 2011[82] adopte la **lettre recommandée électronique**, applicable à tout contrat conclu par voie électronique. Il a introduit un nouvel article : l'article 1369-8 du Code civil. Il a trait uniquement à la conclusion ou à l'exécution du contrat électronique, et uniquement dans le domaine contractuel. L'article 1369-8 du Code civil dispose : « *Une lettre recommandée relative à la conclusion ou à l'exécution d'un contrat peut être envoyée par courrier électronique à condition que ce courrier soit acheminé par un tiers selon un procédé permettant d'identifier le tiers, de désigner l'expéditeur, de garantir l'identité du destinataire et d'établir si la lettre a été remise ou non au destinataire. Le contenu de cette lettre, au choix de l'expéditeur, peut être imprimé par le tiers sur papier pour être distribué au destinataire ou peut être adressé à celui-ci par voie électronique. Dans ce dernier cas, si le destinataire n'est pas un professionnel, il doit avoir demandé l'envoi par ce moyen ou en avoir accepté l'usage au cours d'échanges antérieurs.* ».L'admission de la lettre recommandée électronique est donc soumise à des conditions :

-le courrier doit avoir été acheminé par un tiers ;
-l'expéditeur doit être désigné et l'identité du destinataire garantie ;
-la remise de la lettre au destinataire doit être établie ;
-la date d'expédition et de réception doit être fiable ou présumée fiable selon un Décret qui va être prochainement publié.
Toutes ces exigences permettent d'assurer la même efficacité que la lettre recommandée sur support papier, et d'être sécurisée.

75. Après l'adaptation des règles de forme, comment les règles de preuve sont-elles adaptées à l'écrit électronique ?

[82] Décr. n° 2011-144, 2 févr. 2011, relatif à l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat, JO n° 0029, 4 févr. 2011, p. 2274, t. n° 19 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023513151

B. L'adaptation des règles de preuve

76. Dans un autre ordre d'idées, les **règles de preuve** propres au papier peuvent s'appliquer à la preuve électronique, sauf exceptions :

-le seuil de 1500 euros mis en place s'applique toujours à l'écrit électronique ;
-la règle du double original est presque inutile pour l'informatique (en effet, en général la première sortie papier n'est que la copie de ce que les rédacteurs ont préparé dans le système) ;
-l'original et la copie se confondent en informatique (toutes les traces comme les cookies sont considérées comme des originaux) ;
-la charge de la preuve est la même en informatique que pour les supports papier (c'est au demandeur que revient la charge de la preuve) ;
-sur les cas d'impossibilité de rapporter un écrit : l'impossibilité physique n'a pas de sens en informatique à part un matériel détérioré avec le temps et donc la disparition d'un document faute de possibilité d'accès…Elle peut se rapprocher avec la perte de l'écrit informatique. Cette hypothèse est la plus vraisemblable. Les fichiers informatiques sont vulnérables : détériorations, virus, sabotage…L'impossibilité morale s'applique bien entendu à l'informatique.

77. A l'issue de ces règles, deux questions se posent :

a) Comment prouver un écrit électronique et comment prouver contre celui-ci ?
b) Un acte écrit électronique peut-il remettre en cause un acte sous seing privé ?

78. *a)* En premier lieu pour répondre à cette interrogation on pourrait admettre que la preuve en matière électronique est libre, qu'elle se fait par tous moyens sans faire de distinction entre un acte de commerce, un acte mixte ou un acte civil. En second lieu on pourrait sinon imposer une preuve littérale par référence à l'article 1341 du Code civil. Or il ne faut pas oublier que les machines ne sont pas infaillibles et que l'appréciation des juges aurait toute son importance. En cas de **conflit de preuves**, la solution finalement retenue est médiane. L'article 1316-1 alinéa 2 du Code civil précise que « *La preuve contraire peut être rapportée contre un écrit électronique sur le fondement de présomptions graves, précises et*

concordantes. ». Cet article impose au juge une plus grande vigilance que la preuve par tous moyens. En effet le juge doit prendre en compte des présomptions qui remplissent le caractère de gravité, précision et qui concordent. Il faut savoir dans un premier temps que selon le Code civil, il revient au juge de déterminer quel est le moyen de preuve le plus vraisemblable entre le support écrit et le support électronique en cas de conflit de preuves[83]. Cette règle s'applique lorsque la loi ne prévoit pas d'autres principes et qu'il n'y a pas de convention valable entre les parties. Le même Code prévoit expressément la même force probante entre l'écrit sur support papier et l'écrit sur support électronique.

79. La **preuve de l'écrit sous forme électronique**, acte authentique ou acte sous seing privé est admise dès lors que sont remplies **deux conditions** contenues à l'article 1316-1 du Code civil :

-l'identification claire de la personne dont l'acte émane : « *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose*[84]. » ;
-la conservation et l'établissement de l'acte dans des conditions de nature à en garantir l'intégrité.

80. *b)* En second lieu, l'article 1316-16 alinéa 3 précise que l'écrit électronique ne peut pas prouver contre ou outre un acte sous seing privé signé par les parties. Certains universitaires approuvent cette disposition et d'autres non. C'est le cas du magistrat P. Leclerq qui met en avant l'insécurité des preuves électroniques : « *Les preuves électroniques sont, aujourd'hui encore trop unilatéralement établies et archivées, sans garantie de sécurité parfaite, ni même de détection, contre les risques de fraude, émanant d'employés indélicats voire de tiers intrus*[85]*...* ». Cette disposition peut s'expliquer par le manque de fiabilité des machines qui peuvent être manipulées par une seule partie contre l'autre.

81. En ce qui concerne l'article 1316-2 du Code civil, ce dernier invite le juge à prendre en compte le titre le plus vraisemblable dans le cas d'un conflit de preuve littérale : « *Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, les tribunaux règlent les conflits de preuve littérale en déterminant par tous moyens le titre le*

[83] C. civ., art. 1316-2 et 1316-3
[84] C. civ., art. 1316-4 al 1
[85] P. LECLERQ, *Propositions diverses d'évolutions législatives sur les signatures électroniques,* Dr. Informatique et télécoms., 1998, p. 19 s.

plus vraisemblable. ». Le début du texte « *Lorsque la loi n'a pas fixé d'autres principes* », laisse une marge de manœuvre au législateur pour mettre en place des dispositions liées aux évolutions techniques touchant les modes de communication.

82. On observe ainsi la **multiplication des décisions relatives à la preuve des écrits électroniques** au cours de la seconde moitié de la décennie. Citons un arrêt remarqué pour illustration. Dans une affaire rendue le 30 septembre 2010 par la Première Chambre civile de la Cour de cassation[86], la valeur probatoire des courriers électroniques a été précisée. Elle précise que les conditions de validité d'un écrit électronique et de la signature électronique contenues aux articles 1316-1 et 1316-4 du Code civil doivent être vérifiées par les Juges du fond au sens de l'article 287 alinéa 2 du Code de procédure civile lorsqu'il s'agit d'un acte sous seing privé[87]. Il était en effet important de vérifier que le courrier électronique avait bien été signé électroniquement par les signataires, pour assurer l'identification de l'acte et son intégrité. Néanmoins, force est de constater que la majorité des courriers électroniques n'est pas signée. Il est donc souvent considéré comme un **commencement de preuve par écrit** devant être complété par d'autres preuves, et non comme une preuve parfaite. Et si le courrier a bien été signé, le juge doit vérifier que les conditions applicables aux écrits électroniques sont remplies.

83. La preuve électronique a désormais une place équivalente à la preuve littérale. Comment peut-on se servir de ce moyen de preuve dans la mise en cause de la responsabilité des prestataires ?

[86] Cass. 1ère civ., 30 sept. 2010, n° 09-68.555, F-P+B+I, Michelet c/ Frachebois, JurisData n° 2010-017147

[87] « *Convention écrite établie par les parties elles-mêmes ou par un tiers et qui a été signée par elles ou par une personne qu'elles ont constituée pour mandataire* » ; cf. http://www.dictionnaire-juridique.com/definition/sous-seing-prive.php

Section 2 : La possible mise en cause de la responsabilité des prestataires de services de certification électronique

84. Le régime de responsabilité des PSCE (prestataires de services de certification électronique) relève du droit commun des contrats et de la responsabilité civile. Le régime de responsabilité des prestataires de service était prévu par la Directive de 1999[88] *mais n'a été transposé que par la Loi LCEN de 2004*[89]*. La nature dualiste de la responsabilité des PSCE (§1) et sa mise en œuvre (§2) reposent sur une présomption de responsabilité.*

§ 1 La nature de la responsabilité des PSCE

85. On distingue deux sortes de responsabilité : la responsabilité contractuelle (A) et la responsabilité délictuelle (B).

A. Responsabilité contractuelle

86. Pour ce qui est de la **responsabilité contractuelle** du PSCE **à l'égard du signataire**, leur relation est nécessairement contractuelle puisque leur contrat repose sur un **contrat de location**[90] non exclusive et à titre gratuit, d'un logiciel d'infrastructure de gestion de clefs téléchargé sur Internet. Par ce contrat, le PSCE s'oblige à faire jouir l'utilisateur du logiciel d'infrastructure de gestion de clefs pendant une période déterminée et en général à titre gratuit. Le logiciel d'infrastructure peut être comparé à un logiciel de base de données.

[88] Dir. 1999/93/CE, 13 déc. 1999, préc.
[89] L. n°2004-575, 21 juin 2004, préc., art. 33
[90] Appelé aussi contrat de « louage » par lequel « *une des parties appelée bailleur s'oblige, moyennant un loyer, à faire jouir l'autre partie appelée locataire d'une chose immobilière ou mobilière pendant un certain temps.* » ; cf. G. Cornu, *Vocabulaire juridique*, Association H. Capitant, éd. PUF, Paris, avr. 2007, p. 562

87. Ensuite on peut qualifier de **contrat d'entreprise**[91] les services effectués en contrepartie du prix payé par le signataire pour l'obtention d'un certificat[92]. Le contrat d'entreprise résulte de trois contrats distincts :

-le « contrat utilisateur » qui porte sur les conditions générales d'utilisation des prestations de service de certification ;
-la « politique de certification » qui s'applique au certificat obtenu ;
-le « contrat d'assurance » attaché aux services du PSCE.

88. Cependant leur responsabilité n'est pas engagée s'il est démontré que les prestataires n'ont commis aucune faute intentionnelle ou négligence, ou lorsque l'utilisateur a fait un usage du certificat « *dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux utilisateurs*[93] ». En effet, les limites ne sont appliquées que si elles sont connues des utilisateurs : le terme « accessible » s'entend comme le fait que les limites d'utilisation du certificat sont perçues de façon à éviter toute confusion[94].Le texte n'indique pas les conditions de la **défaillance contractuelle entre l'organisme certificateur et son client**, *i.e* le bénéficiaire de la certification. C'est donc le droit commun qui va s'appliquer. La certification est une prestation de service et est une opération technique sans aléa : l'obligation semble donc être de résultat selon Ph. Le Tourneau[95]. Il peut cependant être inséré une clause limitative de responsabilité.

89. On ne peut envisager le système de signature basé sur la confiance, sans contrepartie des garanties juridiques pour les cas où l'autorité de certification manquerait à ses obligations. La responsabilité du tiers certificateur repose donc sur le certificat, sur son contenu plus exactement. Le certificat émis et sur lequel repose la confiance du système permet de dégager les obligations essentielles du tiers certificateur.

[91] Appelé aussi contrat d' «ouvrage », par lequel « *une personne, nommée locateur d'ouvrage (entrepreneur), s'engage à réaliser un ouvrage déterminé pour une autre personne appelée maître de l'ouvrage qui lui en paye le prix, mais à l'égard de laquelle la première n'est pas en état de subordination juridique*. » ; cf. G. Cornu, *Vocabulaire juridique*, Association H. Capitant, éd. PUF, Paris, avr. 2007, p. 562
[92] Cf. PARTIE II, Chapitre I
[93] L. n° 2004-575, 21 juin 2004, préc., art. 33-4°
[94] E. A CAPRIOLI, *Signature et confiance dans les communications électroniques en droit français et européen*, in Libre droit, Mélanges Ph. Le Tourneau : Dalloz, 2008, p. 55 et s.
[95] PH. LE TOURNEAU, *Droit de la responsabilité et des contrats*, Coll. Dalloz Action, D., 8ème éd. févr. 2010, Paris, p. 912

90. Le **signataire** quant à lui peut voir également sa responsabilité engagée s'il n'a pas gardé sous son contrôle exclusif sa clef privée[96]. On peut alors faire jouer la responsabilité contractuelle si la faute du signataire s'applique dans le cadre du contrat qui le lie au PSCE[97].

B. Responsabilité délictuelle des PSCE

91. Pour ce qui est de la **responsabilité délictuelle** du PSCE **à l'égard des tiers**, ce sont les articles 1382 et 1383 du Code civil qui s'appliquent. Le PSCE se voit engager sa responsabilité si le destinataire qui a signé le document n'est pas valide ou s'il s'est fié au contenu du certificat alors que par exemple la validité du certificat est dépassée ou que l'identité de l'expéditeur n'est suffisamment vérifiée.

92. « *En cas de préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas suivants : les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ; les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ; la délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ; les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu de cette information à la disposition des tiers*.[98] ».

93. Mais comment la responsabilité des PSCE peut être mise en œuvre ?

[96] Décr. n° 2001-272, 30 mars 2001, préc., art. 1er al. 2
[97] L. ASSAYA, *La signature électronique par cryptographie à clef publique*, JCP E. n° 4, 23 janv. 2003, 146, §14
[98] L. n° 2004-575, 21 juin 2004, préc.

§ 2 La mise en œuvre de la responsabilité des PSCE

94. Il faut savoir que les PSCE sont soumis à une **présomption de responsabilité,** pour les préjudices subis par « *les personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés.*[99] ». Le fait que le prestataire présente le certificat comme qualifié est donc déterminant, qu'il réponde aux critères posés par le Décret de 2001[100] ou non. Cette présomption de responsabilité s'applique dans cinq cas :

-inexactitude des informations contenues dans le certificat à la date de la délivrance ;
-présentation d'un certificat comme qualifié alors qu'il ne l'est pas ;
-délivrance d'un certificat pour une signature dont le signataire ne dispose pas des données nécessaires à la création de la signature ;
-défaut d'enregistrement de la révocation d'un certificat et d'information des tiers.

95. La responsabilité s'applique à **trois catégories de prestataires de services** :

-les prestataires intermédiaires[101] : ce sont les fournisseurs d'accès ;
-les hébergeurs de sites[102] dès lors qu'ils n'ont pas effectivement connaissance de l'activité ou d'informations illicites ;
-les personnes assurant les activités de stockage d'informations sous forme de caching[103] (conserver l'information par un fournisseur d'accès ou un tiers de confiance, pour la rediffuser ensuite sur le réseau).

96. Cette présomption de responsabilité est très forte pesant sur les fournisseurs d'accès et sur les personnes assurant le stockage d'informations[104]. Le prestataire de service commettra une faute s'il n'obtempère pas une injonction prononcée par une autorité administrative ou judiciaire. En revanche la présomption est moins forte pour les hébergeurs de sites car ils

[99] L. n° 2004-575, 21 juin 2004, préc., art. 33
[100] Décr. n° 2001-272, 30 mars 2001, préc.
[101] Dir. 1999/93/CE, 13 déc. 1999, préc., art. 12
[102] Dir. 1999/93/CE, 13 déc. 1999, préc., art. 14
[103] Dir. 1999/93/CE, 13 déc. 1999, préc., art. 13
[104] Dir. 1999/93/CE, 13 déc. 1999, préc., art. 12 et 13

doivent prendre des mesures lorsqu'ils ont connaissance d'activités ou d'informations illicites[105].

97. La **victime doit donc prouver la faute** du prestataire pour obtenir réparation, il s'agit d'une « *responsabilité pour faute caractérisée du prestataire qui confine à la faute lourde*[106] » selon L. Grynbaum. Selon le même auteur, c'est dommage de constater que la réparation de la victime n'est pas un objectif principal de la Directive, que la protection du plus faible ne soit pas un objectif primordial. Il montre que la preuve d'une faute caractérisée marque le retour à un individualisme juridique du XIXème siècle[107].

98. Il faut bien distinguer selon que la signature est présumée fiable ou pas. On peut considérer qu'il existe **deux degrés de fiabilité**[108] :

-la **signature électronique simple** dont la fiabilité n'est pas du tout présumée : elle devra être prouvée devant le juge *a posteriori*. Celui qui entend se prévaloir d'une signature électronique simple devra rapporter la preuve du respect par le procédé utilisé des conditions posées à l'article 1316-4 du Code civil, *i.e* « *un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache*. » ;
-la **signature électronique sécurisée** dont la fiabilité est présumée : la valeur juridique est *a priori* reconnue sauf preuve contraire rapportée devant le juge. La présomption de fiabilité, bien que simple, permet de faire bénéficier la signature électronique d'une présomption de conformité aux conditions posées à l'article 1316-1 du Code civil, et peut être admise en preuve au même titre que l'écrit sur support papier jusqu'à preuve contraire.

99. Pour illustrer ce propos dans un contexte international, on peut citer un arrêt rendu par la Chambre criminelle de la Cour de cassation de l'**Etat de New-York** le 27 mai 2008[109], à l'occasion d'une signature électronique présente dans un contrat d'assurance. Cette affaire donne une interprétation intéressante de la validité d'une signature et de la preuve de sa fiabilité. Dans l'Etat de New-York, la signature électronique a la même valeur que la

[105] Dir. 1999/93/CE, 13 déc. 1999, préc., art. 14
[106] L. GRYNBAUM, La directive « commerce électronique » ou l'inquiétant retour de l'individualisme juridique, JCP G., 21 mars 2001, I 307, p. 9
[107] L. GRYNBAUM, La directive « commerce électronique » ou l'inquiétant retour de l'individualisme juridique, 21 mars 2001, préc., p. 9
[108] E. A. CAPRIOLI, *HADOPI et signature électronique des procès-verbaux des agents*, CCE, n° 10, oct. 2010, comm. 104, p. 1
[109] Cass., crim., 27 mai 2008, n° 07-88.176, F-P+F, JurisData n° 2008-044294

signature manuscrite. Au sens d'une Loi de 1999[110], elle doit être entendue comme un son, un symbole ou un procédé électronique, attaché logiquement à un document et réalisée par une personne qui a l'intention de signer ce document. Les magistrats ont décidé que c'est à la partie du contrat voulant faire respecter une signature électronique non sécurisée sur un contrat d'assurance qu'il revient de rapporter la preuve d'authentification de la partie signataire. Ce qui signifie que la fiabilité de la signature électronique simple, portée sur un contrat d'assurance n'est pas présumée. C'est à la partie qui souhaite faire jouer la signature électronique que revient la charge de la preuve.

100. On a vu que la signature électronique est avant tout un mécanisme d'identification et d'engagement, au même titre que la signature manuscrite. Cependant ce n'est pas le seul rôle qu'elle a. Elle assure l'intégrité de l'acte qui la contient. La signature électronique est efficace de par son mécanisme et son rôle. Son fonctionnement via la technique de la cryptographie, et la possibilité d'utiliser la signature en tant que moyen de preuve sont à l'origine de son équivalence avec la signature manuscrite, et de son utilité. Mais un mécanisme efficace ne correspond toujours pas avec l'utilité sécuritaire qu'on peut vouloir lui donner. L'efficacité n'a pas forcément pour corollaire la fiabilité. Or, la signature électronique fait appel à des outils techniques relevant de machines non éternellement utilisables, et surtout elle est ouverte à la fraude. Comment lutter contre ce phénomène répandu en informatique ? Seule la sécurisation permet de répondre à ce problème.

[110] NYS Technology Law, 28 septembre 1999

PARTIE II. LA SECURISATION DE LA SIGNATURE ÉLECTRONIQUE

101. La signature électronique n'est pas seulement un outil d'authentification de l'auteur de l'acte, c'est également un produit de sécurité. La signature a donc une fonction sécuritaire. Comment la sécurisation apporte la fiabilité nécessaire de la signature électronique (Chapitre I). Est-elle la raison de l'extension de son champ d'application (Chapitre II) ?

Chapitre I : La fiabilité de la signature électronique

102. La fiabilité de la signature électronique se situe dans la délivrance d'un certificat dit « carte d'identité électronique » (Section 1), et dans l'équivalence entre la signature électronique et la signature manuscrite (Section 2).

Section 1 : La délivrance de la « carte d'identité électronique »

103. Cette mission impose la participation des prestataires de services de certification électronique (§1) et des autorités de certification (§2).

§ 1 Le rôle des PSCE

104. Les **PSCE** ont un rôle important, ils doivent « *enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par voie électronique, d'utiliser des systèmes fiables pour stocker les certificats*[111]. »Un PSCE

[111] Dir. 1999/93/CE, 13 déc. 1999, préc.

peut **déclarer délivrer des certificats qualifiés**. Il devra l'indiquer lorsqu'il se déclarera auprès de l'ANSSI[112]. De plus, ils peuvent être soumis à un contrôle sur le respect des exigences mentionnées à l'article 6.II du Décret de 2001[113], d'office ou à l'occasion de toute réclamation mettant en cause l'activité d'un PSCE. Si le contrôle révèle que le PSCE ne répond pas à ces exigences, l'ANSSI fera une publicité des résultats du contrôle.

105. Les PSCE peuvent volontairement se soumettre à une évaluation pour être qualifiés. On appelle ça l' « **accréditation volontaire »** selon les termes de la Directive de 1999[114]. Les certificats qu'ils délivrent sont alors présumés qualifiés s'ils proviennent d'un PSCE qualifié. Cependant les PSCE qui n'ont pas reçu d'attestation de qualification peuvent délivrer des certificats qualifiés s'ils estiment eux-mêmes répondre aux exigences de l'article 6.II du Décret de 2001[115]. C'est le COFRAC[116] en France qui est chargé d'effectuer une évaluation avant l'attribution de la qualification des PSCE.

106. Depuis un Arrêté du 7 août 2004[117], sur l'accréditation et la qualification des prestataires de services de certification électronique, un nouveau régime a été mis en place. Il est plus souple et plus précis. En ce qui concerne l'**accréditation**, sa durée n'est plus limitée à deux ans mais à cinq ans. De plus, l'accréditation fait référence à la norme NF EN 45012.[118] L'Arrêté est venu préciser également les exigences techniques permettant l'accréditation et ajoute que les causes de révocation des certificats et les techniques particulières qui concernent la cryptographie sont soumises à la confidentialité. La **qualification** des prestataires, quant à elle, n'est plus limitée à deux ans mais est limitée à trois ans. Enfin, une obligation d'effectuer un **audit de surveillance annuel** a été mis en place.

107. Les PSCE ont également l'obligation de « *conserver, éventuellement sous forme électronique, toutes les informations relatives aux certificats électroniques qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique ou*

[112] Agence Nationale de la Sécurité des Systèmes d'Information, anciennement DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information)
[113] Décr. n° 2001-272, 30 mars 2001, préc., Art. 6.II
[114] Dir. 1999/93/CE du Parlement et du Conseil, 13 déc. 1999, préc., art. 3.2
[115] Décr. n° 2001-272, 30 mars 2001, préc., art. 6-II
[116] Comité Français d'Accréditation
[117] Arr. n° 182, 26 juill. 2004, relatif à la reconnaissance de la qualification des prestataires de services de certification électronique, JO 7 août 2004, p. 14104, t. n° 17 ;
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441678
[118] Label officiel français délivré par l'Association française de normalisation, qui atteste de la conformité aux normes françaises

d'utiliser des systèmes de conservation des certificats qui garantissent que l'introduction de la modification des données est réservée aux seules personnes autorisées à cet effet par le prestataire et que toute modification de nature à compromettre la sécurité du système puisse être détectée.[119] » En effet, si le PSCE demande à être qualifié, il peut exiger d'utiliser des produits certifiés conformes. S'il génère les clefs de l'utilisateur, il devra utiliser un produit évalué et certifié.

108. Le PSCE doit **contrôler l'identité de la personne** à laquelle il délivre le certificat électronique, « *en exigeant d'elle la présentation d'un document officiel d'identité*[120] ». C'est après cette vérification qu'il pourra inscrire l'identité du signataire ainsi que la clef publique de ce dernier dans le certificat électronique à émettre. Un élément important est à connaître : l'identité du demandeur n'est pas nécessairement son nom, ça peut être son pseudonyme ! En effet, il est précisé que le certificat doit comprendre le « *nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel*[121]. ». Le rôle du PSCE est d'authentifier l'identité qui lui est présentée, même s'il s'agit d'un pseudonyme, et non de garantir l'identité du signataire…et même s'il connaît sa véritable identité dans le cas où le signataire ne donne qu'un pseudonyme, puisqu'il a la preuve de son identité grâce à la présentation d'un document officiel d'identité.

109. Selon un auteur, « *Le législateur français établit plus un contrôle en aval, laissant aux prestataires de service le choix de se faire « qualifier » ou non, avec une présence administrative moindre, son but étant d'éviter une trop forte rigidité face aux évolutions technologiques constantes. L'absence de contrôle en amont est-elle source de difficulté ? Rien en effet ne permet d'attester que les produits utilisés sont bien conformes aux exigences légales. Observera-t-on dans ce cas une certaine réticence des professionnels français à utiliser la signature électronique ?* »[122]. Cette citation peut désormais être à nuancer depuis la venue de l'Arrêté de 2004 : il essaie de rendre plus sévère les exigences techniques pour l'accréditation, et a rendu obligatoire un audit de surveillance annuel, qui était jusque-là facultatif. Même si la qualification reste facultative, on peut se demander si on assistera un jour à la qualification obligatoire des prestataires ou à un contrôle en aval renforcé de la part

[119] Décr. n° 2001-272, 30 mars 2001, préc., art. 6-II
[120] Décr. n° 2001-272, 30 mars 2001, préc., art. 6-II-m
[121] Décr. n° 2001-272, 30 mars 2001, préc., art. 6-I
[122] B. JALUZOT, *Transposition de la Directive « signature électronique: comparaison franco-allemande*, D. 2004, p. 2286

de l'administration. Les professionnels n'ont pas de réticence à utiliser une signature électronique qui devient de plus en plus fiable et sécurisée. Son efficacité est telle qu'elle touche de plus en plus de domaines.

110. Les PSCE sont soumis au moins à une autorité de certification mais peuvent être soumis à plusieurs autorités en fonction de son organisation. Elles peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres. Le PSCE est alors identifié grâce à son autorité de certification qui a émis le certificat. *Quel est alors le rôle des autorités de certification ?*

§ 2 Le rôle des autorités de certification

111. C'est une autorité « *chargée par un ou plusieurs utilisateurs de créer et d'attribuer leur clef publique et leur certificat*. [123]». Elles assurent une fonction essentielle parmi d'autres : formaliser le lien qui existe entre une personne physique ou morale et une paire de clefs asymétriques. Parmi les fonctions exercées par les **autorités de certification**, la plus importante est celle de l'**émission de certificats**. Les autorités de certification s'authentifient elles-mêmes en apposant leur signature numérique. Le certificat est produit par une autorité de certification qui s'engage sur la chose en la signant elle-même. Elle a donc un certificat qu'elle a obtenu d'une autre autorité de certification. *« Il y a donc une AC[124] de l'AC ou pour complaire à l'antique sentence de Juvénal, un gardien du gardien,[125]* (…) *qui rappelle la « recherche de la norme juridique fondamentale » dans la théorie générale du droit, chère à Hans Kelsen.».*

112. L'autorité de certification est **accréditée** par une autorité de gestion de la politique. Elle peut ainsi utiliser un certificat renforcé, utilisé par l'opérateur de certification pour signer la clef publique. Cela permet de vérifier l'intégrité par le hachage des données et donc de vérifier que les données n'ont pas été modifiées ; et ça permet également de vérifier que les données proviennent bien de l'émetteur connu.

[123] UIT-T, Annuaire, Cadre d'authentification, Fasc. VIII.8, 1988, art. 10.1.1
[124] Autorité de certification
[125] T. PIETTE-COUDOL, *Une signature électronique altérée vicie-t-elle la procédure dématérialisée ?*, CMP, n° 1, janv. 2011, comm. 5, p. 2

113. Les autorités remplissent également d'autres fonctions liées à la signature numérique comme l'archivage des informations relatives aux certificats, la création des clefs asymétriques indispensables pour la signature, la vérification des signatures numériques…etc. Elles recensent et contrôlent l'utilisation des certificats. Elles possèdent une liste des certificats révoqués. Elles peuvent également remplir des fonctions annexes comme le maintien de bases de données d'informations commerciales sur les entreprises (chiffre d'affaires, activités, parts de marché…) identification et localisation des partenaires commerciaux, enregistrement et horodatation de la transmission et de la réception des messages.

114. Comme autorités de certification on peut en citer deux :

-« Certigna » : « *SuiteCertigna permet à l'internaute de signer, horodater et rendre confidentiel tous ses documents (factures, fiches de paie, contrats…), il permet aussi d'effacer de manière sécurisée les fichiers présents sur son ordinateur*.[126] ».

-« Certeurope » : « *CertSign opère les vérifications indispensables à la signature électronique. CertSign est idéal pour signer des contrats, bons de commande, formulaires, bons pour accord, conditions générales de vente…*»

115. Toutes ces différentes missions qu'exercent les autorités de certification participent à sécuriser et rendre fiable la signature électronique. Mais la fiabilité de la signature passe avant tout par un système élaboré pour rendre la sécurisation possible. C'est le résultat de l'équivalence entre la signature manuscrite et électronique.

[126] Cf. www.dhimyotis.com

Section 2 : L'équivalence entre la signature manuscrite et électronique

116. Cette équivalence se situe dans le mécanisme sécurisé de la signature électronique. Le processus de signature électronique peut être renforcé pour procurer une meilleure sécurité. La sécurisation de la signature électronique passe par trois étapes : le respect des conditions précédemment évoquées, un dispositif sécurisé de création de la signature électronique, qui est contrôlé par un tiers vérificateur et la délivrance d'un certificat électronique. La signature électronique par cryptographie à clef publique a la même valeur probante que la signature manuscrite dans le sens qu'elle est présumée fiable lorsque son dispositif est sécurisé (§1) et que son authenticité est vérifiée grâce à une procédure de certification (§2).

§ 1 Le dispositif de sécurisation de la signature électronique

117. La sécurisation de la signature électronique passe par l'exigence de conditions (A) qui permettent de faire place à une présomption de fiabilité de la signature électronique (B).

A. L'exigence de conditions

118. La signature électronique est équivalente à la signature manuscrite depuis qu'elles ont été portées au même rang. La Directive[127] énonce en effet une « **équivalence automatique** » entre la signature électronique et la signature manuscrite si trois conditions sont réunies : « *Une signature électronique avancée, un certificat qualifié et un dispositif sécurisé de création de signature* ». La signature électronique « avancée » selon la Directive, correspond à la signature électronique sécurisée.

[127] Dir. 1999/93/CE, 13 déc. 1999, préc

119. Tout d'abord, il faut savoir que la signature est un **élément essentiel de la validité d'un acte sous seing privé**, qui est alors manuscrite. Pour que la signature manuscrite ait son équivalent dans le cadre des messages électroniques, la signature électronique est consacrée pour les actes sous seing privé à l'article 1322-1 du Code civil : « *La signature nécessaire à la perfection d'un acte sous seing privé identifie celui auquel il est opposé et manifeste son consentement aux obligations qui en découlent. Elle s'entend de l'apposition de son nom ou d'un autre signe personnel ou de l'usage d'un processus d'identification incorporé à l'acte ou formant un tout avec lui.* ». Ensuite, la signature doit répondre à un besoin de fiabilité et de sécurisation. L'article 1316-4 al 2 du Code civil précise que la signature électronique consiste en « *l'usage d'un procédé fiable d'authentification 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 les conditions fixées par décret en Conseil d'Etat.* ».

120. Elle est donc sécurisée lorsque la signature électronique répond aux exigences de sécurité du commerce électronique. Dans cette hypothèse, la signature électronique est réputée « sécurisée » si la signature respecte trois critères imposés par le Décret de 2001[128]:

-elle est propre au signataire ;
-elle a été créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
-si elle garantit avec l'acte auquel elle se rattache un lien tel qu'une modification ultérieure serait détectable[129].

121. En d'autres termes, la signature électronique doit pouvoir identifier l'auteur de l'acte et garantir l'**intégrité** de l'acte. Concernant le terme « intégrité », il est très peu utilisé en droit. L'intégrité d'une chose signifie que cette chose n'a pas été altérée, modifiée, volontairement ou non. Elle s'applique à la signature électronique dans le sens où le document sur lequel elle est apposée ne doit pas avoir été modifié ou altéré. La signature a un rôle protecteur de ce document. La signature électronique n'est pas seulement un outil d'identification électronique, elle doit répondre à des exigences qui prouvent par la suite sa sécurisation. C'est un outil sécurisé. Elle doit être :

[128] Décr. n° 2001-272, 30 mars 2001, préc.
[129] Décr. n° 2001-272, 30 mars 2001, préc., art. 1er al. 2

-infalsifiable ;
-non réutilisable (elle ne peut pas être utilisée dans un autre document) ;
-inaltérable (le document ne peut plus être modifié) ;
-irrévocable : le signataire ne peut revenir sur sa volonté.

B. La présomption de fiabilité

122. Le Décret de 2001[130] a **recours à deux reprises à la présomption** :

-*la présomption de fiabilité de la signature électronique, si les trois conditions sont remplies* :

-la signature répond à la définition d'une signature sécurisée au sens de l'article 1 du Décret ;
-le dispositif de création de signature a reçu un certificat de conformité aux exigences de l'article 3.I du Décret et dans les conditions énoncées dans l'article 3.II de ce même texte ;
-le **certificat électronique** utilisé pour vérifier la signature comporte les champs énoncés dans l'article 6.I du Décret de 2001 et a été émis par un PSCE respectant les exigences de l'article 6.I du Décret.

-*la présomption de conformité des certificats électroniques aux exigences de l'article 6 (s'il a été émis par un PSCE qualifié) si des conditions sont respectées. Il faut en effet :*

-**une signature « sécurisée »** : la définition de la signature électronique « avancée » a été reprise dans les textes transposant la Directive de 1999.[131] Elle comprend les trois critères précédemment énoncés, « *être liée uniquement au signataire ; permettre d'identifier le signataire ; être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure de données soit détectable*. » ;
-**un dispositif sécurisé de création de signature électronique** : il est précisé que le matériel utilisé pour la création de la signature électronique doit être garanti par « *des moyens techniques et des procédures appropriées, que les données de création de signature électronique ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;*

[130] Décr. n° 2001-272, 30 mars 2001, préc.
[131] Dir. 1999/93/CE, 13 déc. 1999, préc.

ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière satisfaisante par le signataire contre toute utilisation par des tiers. »

123. Le même Décret du 30 mars 2001précise les **conditions** pour que le **dispositif de création** de la signature soit sécurisé :

« *Un dispositif sécurisé de création de signature électronique doit :*

1) *Garantir par des moyens techniques et des procédures appropriées que les données de création de signature électronique :*
   a) *Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;*
   b) *Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;*
   c) *Ne peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.*
2) *N'entraîner aucune altération du contenu à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer*.[132] »

Un dispositif de création de signature électronique complet doit générer des données de création (clef secrète) et de vérification (clef publique) de la signature électronique, et la création de la signature électronique. Les produits évalués sont ensuite soumis à une analyse des mécanismes cryptographiques réalisée par l'ANSSI.

124. La **présomption de fiabilité** prévue à l'article 1316-4 du Code civil entourant la signature électronique montre qu'elle peut avoir un caractère « *technologiquement* » irréfragable[133]. Ce qui diffère de la signature électronique simple c'est que cette dernière ne dispose pas de la présomption de fiabilité. Celui qui entend se prévaloir d'une signature électronique simple devra rapporter la preuve du respect par le procédé utilisé des conditions posées à l'article 1316-4 du Code civil, *i.e* « *un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache*. »

125. Les ***e-mails*** n'échappent pas à la présomption de fiabilité reconnue aux écrits électroniques, si les conditions requises par le Code civil sont respectées. Un arrêt récent illustre ce propos, rendu par la Première Chambre civile de la Cour de cassation en date du 30

[132] Décr. n° 2001-272, 30 mars 2001, préc., Art. 3.I
[133] T. ABALLEA, *Signature électronique, quelle force pour la présomption légale ?*, D. 2004, p. 2235

septembre 2010[134]. Dans les faits, était contestée la fiabilité des messages électroniques. Ces derniers ont été utilisés par un bailleur à l'égard de son locataire pour lui mentionner la date de départ du préavis restant à courir. Le locataire se prévaut de cet *e-mail* pour justifier de l'acceptation par le bailleur de la date de son congé, alors que ce dernier nie être l'auteur du message. Se posait donc la question de savoir si l'*e-mail* bénéficie de la présomption de fiabilité. Les juges du fond dans un arrêt du 2 décembre 2008, répondent par la négative et condamnent le bailleur, sans avoir préalablement vérifié les conditions requises pour admettre un écrit électronique à titre de preuve. La Cour de cassation censure la décision de la Cour d'appel en rappelant les règles en matière de preuve littérale des articles 1316-1 et 1316-4 du Code civil. L'écrit électronique est admis en preuve et bénéficie de la présomption de fiabilité que si sont satisfaites plusieurs conditions : doit être possible l'identification de l'auteur de l'acte, l'acte doit être établi et conservé dans des conditions de nature à en garantir l'intégrité[135] et il doit être revêtu d'une signature électronique. En l'espèce l'*e-mail* ne répondait pas à ces conditions, il n'a pu donc bénéficier de la présomption de fiabilité. Il ne correspondait qu'à un commencement de preuve par écrit.

126. *La signature électronique, pour consister en un processus sécurisé, un procédé fiable d'identification et pour garantir l'acte avec lequel elle s'attache[136], nécessite une certification électronique.*

[134] Cass. civ. 1ère, 30 sept. 2010, n° 09-68555, BICC n° 734, 15 janv. 2011
[135] C. civ., art. 1316-1
[136] C. civ., art. 1316-4

§ 2 La certification de la signature électronique

127. La procédure de certification (A) établit le lien indispensable entre la clef publique et son propriétaire, le signataire. Le certificat électronique (B) offre la concordance entre l'identité du signataire et la clef publique.

A. La procédure de certification

128. Le Décret de 2001[137] précise les conditions permettant la réussite d'une **certification**. La signature électronique doit être certifiée conforme aux **exigences** prévues à l'article 3.I :

-soit par le Premier Ministre chargés de la sécurité des systèmes d'information ;
-soit par un organisme désigné à cet effet par un Etat membre de la Communauté européenne.
Cette procédure se décline en trois étapes :

1 : le prestataire doit formuler une demande de certification auprès de l'ANSSI ;
2 : le prestataire doit ensuite faire évaluer son système par un Centre agréé par le Premier ministre ;
3 : un rapport de certification sera ou non accordé. S'il est accordé c'est pour 2 ans.

129. La procédure de certification doit être **fiable**. Pour cela elle doit répondre à des conditions :

1 : sécurité contre toute intrusion et mauvaise utilisation ;
2 : disponibilité, intégrité et services à un niveau raisonnable ;
3 : adhésion à des principes de sécurité ;
4 : objectifs de confidentialité, intégrité, disponibilité et utilisation légitime.

130. L'**évaluation du dispositif à certifier** doit avoir lieu dans un Centre d'évaluation agréé par l'ANSSII. Il s'appuie sur les critères normalisés : les ITSEC (de moins en moins utilisés)

[137] Décr. n° 2001-272, 30 mars 2001, préc.

ou la norme IS 15408[138]. Cette évaluation permet de certifier la conformité d'un dispositif à une cible de sécurité.

131. L'**ANSSI**[139]a été créée par le Décret du 7 juillet 2009[140] sous la forme d'un service à compétence nationale. Elle est héritière du Service central de la sécurité des systèmes d'information (SCSSI) et de la Direction centrale de la sécurité des systèmes d'information (DCSSI). Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale. C'est donc une autorité nationale. Elle est chargée de proposer des règles à appliquer pour la protection des systèmes d'information de l'Etat et de veiller à l'application des mesures adoptées. Dans le domaine de l'informatique elle est chargée d'assurer un service de veille, de détection, d'alerte, de réaction aux attaques informatiques. Parmi d'autres missions, pour ce qui nous intéresse, elle est chargée de la promotion des technologies, des systèmes et des savoir-faire nationaux. Mais surtout, elle contribue au développement de la confiance dans l'économie numérique.

B. Le certificat électronique

132. Le certificat est la « *pierre angulaire de la signature électronique car il établit la relation entre le signataire et la signature* » selon B. Jaluzot[141]. C'est une « *carte d'identité électronique* »[142] permettant d'établir un lien entre une personne et sa signature électronique. Selon le législateur français, le certificat est un « *document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire.*[143] ». Le certificat est un message électronique délivré par un tiers de confiance qui a pour fonction d'établir un lien entre une personne physique ou morale dûment identifiée et une paire de clefs asymétriques (privée et publique).

[138] Appelée aussi « CC » : critères communs
[139] Cf. www.ssi.gouv.fr
[140] Décr. n° 2009-834, 7 juill. 2009, portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », JO n° 0156, 8 juill. 2009 , t. n° 3 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212
[141] B. JALUZOT, *Transposition de la Directive « signature électronique » : comparaison franco-allemande*, préc.
[142] C. FERAL-SCHUHL, *Cyberdroit : le droit à l'épreuve de l'internet*, 6ème éd., Dalloz, Coll. Praxis Dalloz, Paris 2010
[143] Décr. n° 2001-272, 30 mars 2001, préc., art. 1er, 9

Les fichiers électroniques ne sont pas signés au moyen d'un certificat, mais par un logiciel spécialisé qui a besoin d'une clef cryptographique privée émise par le certificateur.

133. Le certificat contient des **informations relatives à l'utilisateur** comme son nom, adresse, capacité, le nom du tiers émetteur du certificat, la clef publique de l'utilisateur, un numéro de série, ses dates de délivrance et d'expiration. Il est nominatif et doit comporter des mentions obligatoires. Il se rattache à une signature électronique et non à un document. En ce qui concerne les entreprises, il y aura autant de certificats délivrés que de personnes physiques dûment habilitées par cette entreprise à procéder à des signatures électroniques[144].

134. **Sous quelle forme se présente-t-il ?** Le certificat électronique a la forme d'un fichier informatique, conservé éventuellement par le signataire sur son ordinateur. Il peut encore le stocker sur un support externe comme une un CD Rom, une clef USB, une carte à puce avec mot de passe…Son fonctionnement est basé sur le chiffrement d'informations et sur la confiance.

135. **Comment utiliser un certificat ?**Au départ l'utilisation d'un certificat se fait en mode non sécurisé (http). C'est la première étape utilisée entre un client et un serveur avant l'ouverture d'une connexion en mode sécurisée (https). Ensuite, le mode sécurisé se met en place avec la clef de chiffrement et la clef de signatures. La clef de chiffrement est celle de l'émetteur et du destinataire, gérée par le navigateur. La clef de signatures est la clef temporaire créée par l'émetteur à partir de la clef publique du destinataire et des clefs du certificat de l'autorité de certification.

136. Un certificat peut être **qualifié**. Il est reconnu comme tel s'il est conforme aux exigences du Décret de 2001[145] et s'il est fourni par un prestataire de service de certification électronique qui répond également aux conditions du même Décret[146].Ces mentions obligatoires sont :

[144] S. STAUB, *Mode d'emploi pour une mise en place réussie de la signature électronique*, Option Finance, n° 701, 2 sept. 2002, p. 35
[145] Décr. n° 2001-272, 30 mars 2001, préc., Art. 6.I
[146] Décr. n° 2001-272, 30 mars 2001, préc., Art. 6.II

-indication que ce certificat est délivré à titre de certificat électronique qualifié ;
-identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;
-nom du signataire ou pseudonyme ;
-données de vérification de signature électronique (données de création) ;
-certificat électronique ;
-signature sécurisée du prestataire de services de certification électronique ;
Certaines mentions ne sont que facultatives, c'est le cas par exemple de l'indication des conditions d'utilisation du certificat électronique.

137. Le certificat est censé être « **conforme** » s'il n'a pas été révoqué avant la fin de sa période normale de validité (un an). Le certificat peut être révoqué à la demande du propriétaire, « *sans délai et avec certitude*[147] ». La **qualification** est cependant valable pour un an. Elle doit être renouvelée à la demande du propriétaire. L'utilisation du terme « qualification » par le droit français peut prêter à confusion puisqu'il fait croire que le certificat doit être qualifié par un prestataire qualifié. Or le prestataire n'a enfin pas besoin d'être qualifié pour délivrer un certificat. La certification et la qualification (éventuelle) sont deux moyens de prouver la sécurisation de la signature électronique.

138. Se pose la question de savoir si la **validité** d'un **certificat** peut être remise en cause, dans le cas où il altérerait la signature électronique. Cette problématique a fait l'objet d'un contentieux. Dans un Jugement rendu par le Tribunal administratif de Limoges le 12 novembre 2010[148], le juge a marqué une différence entre le certificat et la signature électronique. En l'espèce la validité du certificat était mise en cause. Le juge considère que tant que l'existence du certificat n'a pas été remise en cause, la mise en cause de la validité du certificat est indifférente. La signature qui en résulte n'est donc pas altérée et est tout à fait valable. Les documents administratifs en l'espèce étaient donc considérés comme signés, valables et garantis dans leur intégrité.

139. On peut noter qu'il existe des **classes de certificats** dans l'offre des certificateurs. Ces derniers disposent d'une gamme plus ou moins importante de certificats à leur catalogue dont chaque classe détient une identification plus ou moins précise du demandeur du certificat.

[147] Décr. n° 2001-272, 30 mars 2001, préc., art. 6, II, *c*
[148] TA Limoges, 12 nov. 2010, Infostance c/ Région Limousin et a. ; cf.

Quand un demandeur demande un certificat, il choisit sa classe. Le certificat indique lui-même, parmi ses mentions internes à quelle classe il appartient.

140. Citons un **exemple d'offre commerciale d'une société américaine VeriSign**, cela va permettre d'avoir une vision concrète de l'application des certificats. Cette société américaine présente une typologie de trois classes différentes :

-les certificats de classe 1 : appliqués aux messageries personnelles, ils indiquent le nom déclaré de l'utilisateur et son adresse e-mail. Ils apportent une sécurité relative et assurent un simple contrôle sur la non ambigüité du nom de la personne dans le fichier des porteurs de VeriSign et une simple vérification de l'adresse e-mail.
-les certificats de classe 2 : sont utilisés seulement par les personnes et confirment que les informations d'identité fournies par l'utilisateur ne sont pas en contradiction avec les informations présentes dans les bases de données publiques courantes. Ils sont utilisés pour les e-mails inter ou intra entreprises, messageries personnelles et individuelles, changements de mot de passe et services de souscription en ligne.
-les certificats de classe 3 : délivrés aux personnes physiques et morales, elles demandent la présence physique d'une personne devant une autorité d'enregistrement et utilisent des procédés ayant valeur probante de l'identité des signataires individuels. Pour les entreprises, ces certificats assurent une garantie sur l'existence et la dénomination des personnes morales. Ces certificats sont surtout utilisés dans le commerce électronique.

141. Face à un tel succès dans son mécanisme, la signature fait de plus en plus sa place. Elle s'étend dans de nombreux domaine, que ce soit en droit interne ou international. Si l'usage de la signature électronique a d'abord été conçu comme facultatif, il devient de plus en plus obligatoire dans un nombre croissant de domaines.

Chapitre II : L'extension du champ d'application de la signature électronique

142. La signature électronique voit son application s'étendre de plus en plus en droit interne (Section 1,) et à l'étranger (Section 2).

Section 1 : L'extension de la signature électronique en droit interne

143. Plusieurs domaines touchent désormais l'écrit électronique et la signature électronique, de près ou de loin, en France. C'est le cas notamment en droit cambiaire (§1), dans le secteur Administratif (§2), dans les Sociétés anonymes (§3). L'écrit électronique est utilisé dans les procédures judiciaires (§4) et on observe enfin la dématérialisation récente des actes authentiques (§5).

§ 1 L'écrit électronique et le droit cambiaire

144. La Loi du 13 mars 2000[149] suscite des interrogations en consacrant la signature électronique : on se demande si cette consécration ne peut être étendue en droit cambiaire. La doctrine se pose la question de savoir si on peut parler d'une « ***disparition progressive des mentions manuscrites*** »[150]. La réponse n'est pas si évidente que ça pour ce qui touche au droit cambiaire.

[149] L. n° 2000-230, 13 mars 2000, préc.
[150] C. MALECKI, *Regards sur le formalisme cambiaire à l'heure de la signature électronique*, JCP E., n° 51, 21 déc. 2000, p. 2036, §1

145. En ce qui concerne les **effets de commerce**, certains ont déjà la forme électronique. On peut rappeler un arrêt très remarqué rendu par la Chambre commerciale de la Cour de cassation du 2 décembre 1997[151] concernant le Bordereau Dailly. Ce dernier peut être « *établi ou conservé sur tout support, y compris par télécopies, dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées, ou ne sont pas contestées* ».Cette décision pousse à se demander si elle n'est pas à l'origine d'un véritable bouleversement futur éventuel, menant à l'acception de l'électronique pour les autres effets de commerce. Même si certains effets de commerce ont déjà la forme électronique, il est impossible de renier le formalisme omniprésent, ce qui peut poser quelques problèmes pour l'électronisation de ces effets de commerce.

146. Mais en ce qui concerne les **mentions obligatoires**, celles-ci sont graduées. On peut citer par exemple la possibilité pour le cédant de signer de façon non manuscrite le Bordereau Dailly alors que cette possibilité est interdite au cédé, qui ne doit l'accepter qu'en la forme manuscrite. De plus, la signature manuscrite a un rôle particulier pour les effets de commerce : elle a surtout vocation à garantir l'identification de la personne (donc elle a une force probante). Elle ne s'approprie pas l'acte lui-même, elle ne lui est pas « substantielle », étant donné que l'effet de commerce a vocation à circuler. Aujourd'hui il faut tout de même admettre que le support papier laisse place au support informatisé. Il existe désormais la lettre de change relevée (LCR) magnétique, le billet à ordre relevé et le Bordereau Dailly magnétique. La signature électronique peut alors jouer un rôle important, celui de concrétiser le transfert de la créance, identifier l'auteur de l'effet de commerce et prouver la manifestation de son consentement pour ce qui est de ces effets de commerce. On pourrait également admettre que les mentions obligatoires portées sur les effets de commerce puissent être exprimées mécaniquement, soit par sigle, clef informatique, code… ?

147. La Loi du 13 mars 2000[152] entraîne donc la question de savoir si la signature électronique pourrait s'appliquer aux effets de commerce type LCR ou BOR. Cependant, la réponse ministérielle du 30 novembre 2000[153] semble exclure cette possibilité à cause au formalisme substantiel incontournable qui régit le droit cambiaire et les effets de commerce.

[151] Cass. com., 2 déc. 1997, JCP G. 1998, II, 10097, note Grynbaum; JCP E. 1998, n° 5, p. 178, note T. Bonneau, préc.
[152] L. n° 2000-230, 13 mars 2000, préc.
[153] Rép. min. n° 25110, JO Sénat, 30 nov. 2000

Les commentateurs précisent en effet que la Loi du 13 mars 2000[154] « *ne peut avoir pour effet direct et immédiat de lui conférer des effets juridiques équivalents à la lettre de change, notamment en ce qui concerne les recours cambiaires.* »

148. Qu'en est-il de la signature électronique dans l'Administration ?

§ 2 La signature électronique et l'Administration

149. La Loi du 30 avril 1983[155] et son Décret du 29 novembre 1983[156] ont mis en œuvre la **comptabilité informatisée**. La Loi de finance de 1990[157] a permis la dématérialisation de la facture. La Loi de finance de 1990 institue également une obligation pour les entreprises dont le chiffre d'affaire dépasse 15 millions d'euros et 760 000 pour la TVA d'utiliser la voie électronique pour leur déclaration.

150. La Loi Madelin du 11 février 1994[158] généralise l'obligation pour les entreprises de remplacer toute déclaration écrite avec l'Administration par un message électronique équivalent. De plus, une Ordonnance est venue encadrer les **échanges électroniques entre les usagers du secteur public et l'Administration**. Il s'agit de l'Ordonnance du 8 décembre 2005[159]. Cette dernière met sur le même rang le support écrit et le support électronique dans ce type de relation. Un référentiel général de sécurité (RGS) a été créé et publié conformément à l'Ordonnance du 8 décembre 2005. Il énumère les trois enjeux en matière de

[154] L. n° 2000-230, 13 mars 2000, préc.
[155] L. n° 83-1020, 30 avr. 1983, relative à la mise en harmonie des obligations comptables des commerçants et de certaines sociétés avec la IVè directive adoptée par le conseil des communautés européennes le 25 juillet 1978, JO 3 mai 1983; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068787
[156] D. n° 83-1020, 29 nov. 1983, pris en application de la loi n° 83-353 du 30 avril 1983 et relatif aux obligations comptables des commerçants, JO 1er déc. 1983, p. 3461;http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B1B3406D8FB57C220A5FFFB5A0E63282.tpdjo06v_1?cidTexte=JORFTEXT000000520693
[157] L. n° 901168, 29 décembre 1990, de finances pour 1991, JO 30 déc. 1990 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000717191
[158] L. n° 94-126, 11 févr. 1994, relative à l'initiative et à l'entreprise individuelle, JO 13 févr. 1994, p. 2493, dite Loi Madelin ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000165840
[159] Ord. n° 2005-1516, 8 déc. 2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232 , ratifiée par L. n° 2009-526, 12 mai 2009, de simplification et de clarification du droit et d'allègement des procédures, JO n° 0110, 13 mai 2009, p. 7920; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020604162

sécurité des données et systèmes dans les échanges électroniques et édicte des règles les concernant:

-disponibilité ;
-intégrité ;
-confidentialité.

151. Ce qui est intéressant ici, c'est surtout la **consécration de l'utilisation de la signature électronique sur les actes des autorités administratives** : « *Les actes des autorités administratives peuvent faire l'objet d'une signature électronique. Celle-ci n'est valablement apposée que par l'usage d'un procédé, conforme aux règles du référentiel général de sécurité mentionné au I de l'article 9, qu'il permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de l'acte*[160]. » La signature électronique n'est donc pas seulement réservée qu'aux seuls actes privés, ce qu'avait suggéré la Directive de 1999[161]. Les autorités administratives concernées sont l'Etat, mes collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant les régimes de protection sociale et ceux chargés des services publics administratifs.

152. Quand la signature électronique doit-elle être **sécurisée** ? C'est en fonction de l'objet de l'acte administratif que la signature électronique devra être plus ou moins sécurisée. Dans ce cas ce n'est plus le Décret de 2001[162] qui s'applique mais le RGS pour les actes administratifs. La signature électronique confère alors à l'acte administratif son existence juridique, et son altération ou son caractère incomplet peut faire vicier l'acte d'un vice de forme.

153. Le recours à la signature électronique est aussi présent dans les sociétés ou les entreprises :

[160] Ord. n° 2005-1516, 8 déc. 2005, préc., art. 8
[161] Dir. 1999/93/CE du Parlement et du Conseil, 13 déc. 1999, préc.
[162] Décr. n° 2001-272, 30 mars 2001, préc.

§ 3 Le recours à l'écrit électronique dans la société et l'entreprise

154. Plusieurs modifications ont été mises en place pour élargir l'utilisation de l'écrit électronique en droit des sociétés. C'est le cas notamment des bulletins de paie informatisés (A), la télédéclaration (B) et la télécommunication dans les Sociétés anonymes (C).

A. Le bulletin de paie informatisée

155. La Loi du 12 mai 2009[163] a modifié les articles L. 3243-2 et L. 3243-4 du Code du travail. Ces derniers prévoient désormais la possibilité d'instaurer des **bulletins de paie dématérialisés** dont peuvent avoir accès les salariés avec leur accord, en remplacement des bulletins de paie papier : « *Avec l'accord du salarié concerné, cette remise peut être effectuée sous forme électronique, dans des conditions de nature à garantir l'intégrité des données. Il [l'employeur] ne peut exiger aucune formalité de signature ou d'émargement autre que celle établissant que la somme reçue correspond bien au montant net figurant sur ce bulletin*[164]. ». Cependant cette possibilité doit respecter deux conditions :

-l'employeur est tenu d'en conserver une copie pendant cinq ans ;
-l'écrit électronique doit être conservé dans des conditions qui permettent de garantir l'intégrité des données.

156. La Loi ne précise pas la **forme du consentement** requis du salarié ni le processus de remise électronique. On suppose alors que le consentement du salarié peut être fait par tout moyen, soit écrit soit oral, et la remise de l'écrit peut être faite par intranet de l'entreprise ou bien par adresse électronique. Il s'agit d'une option pour le salarié d'obtenir sa fiche de paie sous la forme électronique, dont la durée n'est pas précisée par la Loi.

[163] L. n° 2009-526, 12 mai 2009, préc., cf. supra note 74
[164] C. Trav., art. L. 3243-2

B. La télédéclaration fiscale des entreprises

157. En ce qui concerne la **TVA**, depuis le 10 février 2002, les personnes assujetties à la TVA peuvent déposer leur déclaration par le site du Ministère des Finances. A partir du 1er avril 2009, le dépôt de la déclaration de TVA des entreprises doit être fait obligatoirement par la voie électronique. Au départ, seules les grandes entreprises dont le chiffre d'affaires réalisé au cours de l'année 2005 était supérieur au montant de 50 m€ hors-TVA étaient tenues de déclarer leur TVA électroniquement. Depuis le 1er juillet 2007, s'est ajoutée à cette obligation leur déclaration mensuelle. Ensuite, à partir du 1er février 2008, les entreprises moyennes qui devaient des déclarer leur TVA mensuelle doivent désormais le faire par la voie électronique.

158. Depuis le 1er janvier 2009, avec la Loi du 30 décembre 1999[165], l'obligation concerne toutes les entreprises. Elles ont l'obligation de déclarer et de payer en ligne la TVA. La signature manuscrite n'étant plus possible, l'authentification du déclarant doit s'effectuer au moyen d'une signature électronique.

C. La télécommunication dans les Sociétés anonymes

159. Un autre point important est intervenu récemment. Il s'agit de l'utilisation de l'écrit électronique et de la signature électronique pour la préparation et la tenue des conseils et assemblées des sociétés anonymes. En effet, le Décret du 11 décembre 2006[166] est venu apporter des modifications dans ce domaine. La télécommunication ou la visioconférence peut être utilisée lors des conseils d'administration ou conseils de surveillance et lors des assemblées générales. Pour ce qui concerne la **convocation aux assemblées générales**, le Décret du 23 mars 1967 prévoyait déjà qu'elle doit contenir l'adresse électronique où peuvent être adressées les questions écrites[167]. En cas de **procuration par voie électronique**,

[165] L. n° 99-1173, 30 déc. 1999, de finances rectificative pour 1999, art. 41, insérant CGI, art. 1649 quater B quater et 1695 quater, JO n° 303, 31 déc. 1999, p. 19968 ;
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000580717
[166] Décr. n° 2006-1566, 11 déc. 2006, modifiant le Décr. n° 67-236 du 23 mars 1967 sur les sociétés commerciales, JO 12 déc. 2006 ;
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000423792
[167] Décr. n° 67-236, 23 mars 1967, préc., art. 123 et 124, devenus C.com, art. R. 225-66 et R. 225-67

s'appliquant à un actionnaire souhaitant être représenté à l'assemblée, elle doit être revêtue de la signature électronique de l'actionnaire ou si les statuts le prévoient, d'une signature réalisée par tout autre procédé répondant aux conditions fixées par le Décret de 1967[168]. Cette disposition n'est pas applicable à la première assemblée générale convoquée après le 1er janvier 2007[169]. L'actionnaire a également la possibilité d'utiliser un **formulaire électronique de vote à distance** qui doit être reçu par la société jusqu'à la veille de l'assemblée générale, au plus tard à 15 heures, heure de Paris, et doit contenir les mentions prévues par les Décrets de 1967 et 2006[170]. Le formulaire de vote à distance doit contenir la signature électronique de l'actionnaire ou une signature réalisée par un autre procédé répondant aux conditions fixées par les mêmes Décrets. Cette disposition n'est également pas applicable à la première assemblée générale convoquée après le 1er janvier 2007[171].

160. D'autres possibilités d'utiliser la voie électronique s'offrent aux actionnaires des SA : l'envoi de questions écrites ou encore les demandes d'inscription par les actionnaires de résolutions à l'ordre du jour de l'assemblée.

161. Le Décret de 2006 précise la **nature de la signature électronique** qui se situe sur la procuration ou le formulaire de vote. Il s'agit soit d'une signature sécurisée[172] ou bien simple[173]. A défaut de stipulation, c'est la signature sécurisée qui s'applique automatiquement.

162. Selon Catherine CATHIARD, « *L'utilisation des moyens de communication électroniques facilite incontestablement l'organisation et la tenue des réunions sociales*.[174] »En effet, la présence physique n'étant plus requise, cela apporte un gain de temps incontestable, un confort pour l'actionnaire et une rapidité sécurisée des opérations. On serait tenté de croire qu'il s'agit d'une ère presque totalement virtuelle, même dans les relations intra sociétaires, voire de la science-fiction qui devient réelle…

[168] Décr. n° 67-236, 23 mars 1967, préc., art. 132, devenu C.com, art. R. 225-79
[169] Décr. n° 2006-1566, 11 déc. 2006, préc., art. 96
[170] Décr. n° 67-236, 23 mars 1967, préc. ; Décr. n° 2006-1566, 11 déc. 2006, préc.
[171] Décr. n° 2006-1566, 11 déc. 2006, préc., art. 96
[172] Cf. infra, PARTIE II, Chapitre I, Section 2
[173] Cf. supra, PARTIE I, Chapitre I, Section 2 ; Signature résultant de l'utilisation de tout procédé fiable d'authentification de l'actionnaire
[174] C. CATHIARD, *L'utilisation des moyens de télécommunication pour la préparation et la tenue des conseils et assemblées des sociétés anonymes*, JCP E., n° 20, 17 mai 2007, 1660, p. 4, §24

163. La signature électronique atteint également les procédures judiciaires :

§ 4 Le recours à l'écrit électronique dans les procédures judiciaires

164. Dans un premier temps, le **Conseil National des Barreaux** et la **Chancellerie** ont conclu des conventions qui ont instauré un intranet sécurisé en 2004, un réseau privé virtuel de la justice (RPVJ) et un réseau privé virtuel des avocats (RPVA) en 2005[175], dans des conditions de sécurité. Ce système permet aux avocats de consulter leur dossier informatique et l'échange électronique des informations concernant les **procédures civiles et pénales**. *Ces réseaux se mettent en place dans les activités des professions judiciaires, ce qui entraine une certaine concrétisation de la signature électronique, que ce soit en matière civile (A) ou pénale (B).*

A. La procédure civile et la signature électronique

165. L'échange électronique se généralise dans les Tribunaux de grande instance par une convention du 28 septembre 2007 entre le Conseil National des Barreaux et la Chancellerie et en matière pénale. Une autre convention a été conclue le 16 juin 2010. Celle-ci a étendu la communication électronique en matière civile dans les Cours d'appel. Ensuite plusieurs textes sont venus ajouter des possibilités de recourir à l'échange électronique entre les cabinets d'avocats et les juridictions. D'abord est apparu un Décret du 9 décembre 2009[176], venu apporter la possibilité à compter du 1er janvier 2011, de communiquer les déclarations d'appel et les constitutions au Greffe par voie électronique, à peine d'irrecevabilité relevée d'office. Ensuite, le Décret du 29 avril 2010[177]prévoit que l'identification réalisée lors de la transmission des actes de procédure transmis aux juridictions par voie électronique vaut signature. Cette disposition est valable jusqu'au 31 décembre 2014 : « *Vaut signature, pour*

[175] Circ., 20 juill. 2009, relative au changement de titulaire du marché, BO min. Justice, 30 oct. 2009, justice 2009/5, texte 1/29, p. 2

[176] Décr. n° 2009-1524, 9 déc. 2009, relatif à la procédure d'appel avec représentation obligatoire en matière civile, JO 11 déc. 2009, p. 21396, t. n° 8 ;
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021446521

[177] Décr. n° 2010-434, 29 avril 2010, relatif à la communication par voie électronique en matière de procédure civile, JO 2 mai, texte n° 17

l'application des dispositions du Code de procédure civile aux actes que les auxiliaires de justice assistant ou représentant les parties notifient ou remettent à l'occasion des procédures suivies devant les juridictions des premier et second degrés, l'identification réalisée, lors de la transmission par voie électronique, selon les modalités prévues par les arrêtés ministériels pris en application de l'article 748-6 du Code de procédure civile [178]». Enfin, un Arrêté du 5 mai 2010[179] ajoute des précisions sur la garantie, la sécurité de transmission des informations échangées par voie électronique. Cela concerne notamment la forme des actes de procédure et la confidentialité des informations. Il précise les conditions de forme des actes de procédure remis par la voie électronique, les modalités du système de communication électronique des juridictions, les modalités concourant à la sécurité des moyens de communication électronique des auxiliaires de justice, les conditions entourant l'identification des parties et les conditions concourant à la sécurité des transmissions.

166. Selon E. A CAPRIOLI, l'avènement d'un texte pour chaque degré ou chaque juridiction risque de créer des problèmes de cohérence et de sécurité, ainsi qu'un alourdissement de la charge de travail des professionnels[180]. Le greffier a par exemple le devoir de vérifier que ce qui figure sur la forme électronique est bien identique à celle qui était présenté sous la forme papier[181]. Il doit aussi conserver l'ensemble des informations relatives aux extraits et certificats qu'il établit, dans un répertoire sur support électronique. Il doit mentionner la date, la nature, le nom des destinataires des documents et le support sur lequel ils sont établis. Les extraits et les certificats doivent être revêtus de la signature électronique sécurisée du greffier qui les a dressés[182].

[178] Décr. n° 2010-434, 29 avril 2010, préc., art. 1er
[179] Arr. 5 mai 2010, relatif à la communication par voie électronique dans les procédures sans représentation obligatoire devant les Cours d'appel, JO 15 mai 2010, p. 9041
[180] E. A. CAPRIOLI, *La signature électronique dans les communications par voie électronique en matière de procédure civile*, CCE n° 7, juill. 2010, comm. 80, p. 2
[181] Décr. n° 2009-1150, 25 sept. 2009, relatif aux informations figurant sur les registre du commerce et des sociétés, JO 30 sept. 2009, p. 15840, t. n° 14, art. R. 123-101-1 ; http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021087520
[182] Décr. n° 2009-1150, 25 sept. 2009, préc., art. R. 123-152-2

B. La procédure pénale et la signature électronique

167. Un Décret du 18 juin 2010[183], à la suite de l'entrée en vigueur de la Loi du 12 mai 2009[184], est venu préciser les modalités d'application de l'article 801-1 du Code de procédure pénale. Cet article autorise l'utilisation de la signature électronique et numérique lors d'une procédure pénale. Ce Décret s'applique aux magistrats, aux avocats et autres professionnels qui participent à une procédure pénale. L'article 801-1 du Code de procédure pénale prévoit que « *Tous les actes mentionnés au présent code, qu'il s'agisse d'actes d'enquêtes ou d'instruction ou de décisions juridictionnelles, peuvent être revêtus d'une signature numérique ou électronique,* (…) »

168. D'autres articles ont été insérés dans le Code de procédure pénale pour préciser l'article 801-1 du même Code. Il est prévu en effet que « *Les actes mentionnés à l'article 801-1 peuvent être revêtus de la signature électronique ou de la signature numérique des personnes concourant à la procédure au sens de l'article 11 et des avocats. Lorsqu'elles sont appelées à signer ces actes, les personnes autres que celles visées au premier alinéa peuvent y apposer une signature numérique.*[185] ».On peut y voir la **consécration des deux signatures**, électroniques (*i.e* sécurisée) et numériques. La signature numérique est ici envisagée comme une signature manuscrite conservée de manière numérique. Le mot employé fait donc référence à la signature numérisée appelée encore scannérisée[186]. Ce qui peut prêter à confusion. Peut se poser la question également du support de la signature numérique : s'agit-il d'un 'scan' ou bien de l'apposition de la signature sur une tablette graphique ?

169. L'émergence de la signature électronique offre le choix des outils pour les professionnels, sauf la signature numérique qui ne peut être utilisée que pour les procédures pénales. Cette possibilité est à féliciter car elle apporte un certain dynamisme et une opérationnalité. Cependant certains auteurs ne sont pas tous de cet avis positif. Ils craignent l'émergence consécutive de nouveaux vices de procédure relatifs au procès-verbal d'audition

[183] Décr. n° 2010-671, 18 juin 2010, relatif à la signature électronique et numérique en matière pénale et modifiant certaines dispositions de droit pénal et de procédure pénale, JO 20 juin 2010, page 11183, t. n° 4 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022363168
[184] L. n° 2009-526, 12 mai 2009**,** de simplification et de clarification du droit et d'allègement des procédures, JO n° 0110, 13 mai 2009, p.7920, t. n° 1 ;
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020604162
[185] C. proc. pén., art. R. 249-9 et s.
[186] Cf. supra, PARTIE I, Chapitre I, Section 2, I

ou relatifs à la fiabilité du procédé utilisé. E. A Caprioli parle de « *surenchère technologique* » qui se fait « *au détriment du bon sens économique et organisationnel* ».

170. Qu'en est-il des actes authentiques ?

§ 5 La dématérialisation des actes authentiques

171. La dématérialisation des **actes authentiques** et de leur signature est prévue par la Loi du 13 mars 2000[187], aux articles 1316-4 et 1317 du Code civil. Cette consécration met sur le même rang les actes sous seing privé et les actes authentiques. Il s'agit par exemple des actes passés par les notaires, les préfets, les huissiers. Le Décret du 10 août 2005 impose la signature par voie électronique de l'acte dressé par les huissiers de justice sur support dématérialisé[188]. Mais il reste neutre sur la technique à utiliser. Est donc prise en compte la signature électronique à clef publique.

172. **Trois conditions** doivent être respectées pour l'établissement et la conservation des actes authentiques, exigées par deux Décrets du 10 août 2005[189] :

-agrément obligatoire par le Conseil supérieur du notariat pour les notaires et par la Chambre ; nationale des huissiers de justice pour les huissiers concernant le système d'exploitation de traitement et de transmission de l'information : garantit l'intégrité de l'acte et la confidentialité du contenu de l'acte ;
-procédé de signature électronique sécurisé pour la signature électronique ;
-conservation de l'acte dans des conditions de nature à en garantir l'intégrité et la lisibilité avec la mise en place d'un « minutier central ».

[187] L. n° 2000-230, 13 mars 2000, préc.
[188] Décr. n° 2005-972, 10 août 2005, modifiant le décret n° 56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice, JO 11 août 2005, p. 13095, art. 26 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000812471
[189] Décr. n° 2005-972, 10 août 2005, préc., et Décr. n° 2005-973, 10 août 2005, modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, JO 11 août 2005, p. 13095 ; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000451599

173. Le Conseil supérieur du notariat devient une autorité de certification électronique le 20 août 2007[190]. Les notaires disposent d'une clé REAL (USB) pour garantir l'authenticité de leur signature électronique.

174. La **première signature d'un acte authentique** a eu lieu le 28 octobre 2008, suivi du premier acte de vente dématérialisé entre deux particuliers sur une parcelle de terrain. Il s'agissait en l'espèce d'une **signature numérisée** des deux parties. Ces dernières ont apposé leur signature à l'aide d'un stylet sur l'écran tactile ou le Tablet PC mis à leur disposition. Le notaire a ensuite apposé sa signature, électronique et sécurisée. Dans un discours du 28 octobre 2008 prononcé devant le Conseil supérieur du notariat (CSN) à l'occasion de la signature du premier acte authentique sur support électronique, Mme Rachida Dati a apporté des précisions sur le développement des nouvelles technologies en Justice, et notamment la possibilité pour le justiciable d'adresser des demandes aux juridictions en ligne, ou bien la dématérialisation des injonctions de payer, ou encore la création d'un groupement d'intérêt public pour permettre une avancée plus rapide de la signature électronique[191].

175. L'acte d'huissier est à la fois un acte de procédure soumis au Code de procédure civile et un acte authentique soumis au Code civil. L'Arrêté du 17 juin 2008[192] a introduit la **possibilité de signifier électroniquement les actes entre avocats au Conseil d'Etat et à la Cour de cassation**. La première signification a été effectuée en décembre 2009 par Maître Saragoussi. Ici c'est l'électronique qui s'est adapté au droit puisqu'il a été mis en place tout en respectant les fondamentaux procéduraux. C'est juste le support qui change et qui devient électronique. Comment se déroule le **processus** ?

-l'avocat met le document à signifier sur le serveur des avocats aux Conseils ;
-le serveur transmet de manière sécurisée le document signé par l'avocat sur le serveur des huissiers audienciers ;
-l'officier public vérifie trois éléments : que le document n'a pas été altéré, que la signature porte sur l'intégralité du document et que l'expéditeur est bien certifié[193] ;

[190] Décr. n° 2005-973, 10 août 2005, préc.
[191] L. DARGENT, *Nouvelles technologies et justice*, D., 30 oct. 2008
[192] Arr. 17 juin 2008, portant application anticipée pour la procédure devant la Cour de cassation des dispositions relatives à la communication par voie électronique ; JO n° 0148, 26 juin 2008, p. 10259, t. n° 27 http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000019066574
[193] Cf. infra, PARTIE II, Chapitre I, Section 2, II

-l'huissier contresigne ensuite le document à signifier, le remet sur le serveur des huissiers audienciers ;
-la procédure est validée si l'acte est intègre, puis un « exploit de signification » est signé par l'huissier et transmis sur le serveur des avocats.

176. La signature électronique de l'officier public authentifie le document et marque la manifestation de la volonté. Elle a le même rôle que la signature manuscrite.Au final, la signification est certes dématérialisée mais elle est sécurisée et intègre.

177. *La dématérialisation prend de l'ampleur en droit interne de manière exponentielle. Mais qu'en est-il en Europe et dans le Monde ? La généralisation progressive de l'écrit électronique et de la signature électronique ne se voit-elle qu'en France ? La Directive de 1999 sur la signature électronique*[194] *introduit déjà la signature électronique au niveau européen, encore faut-il qu'elle soit signée par tous les Etats membres.*

[194] Dir. 1999/93/CE, 13 déc. 1999, préc.

Section 2 : L'extension de la signature électronique à l'étranger

178. La signature électronique est utilisée également dans d'autres pays. Il semble intéressant de comparer leur application à celle de la France : en Europe (§1) et en dehors de l'Europe (§2).

§ 1 L'état des lieux européens

179. Qu'en est-il de la place de la signature électronique en Europe ? (A) L'Allemagne parait être un bon exemple de comparaison avec la France, ayant toutes les deux transposé la Directive de 1999[195] (B).

A. Le développement de la signature électronique en Europe

180. Le **développement** de la signature électronique en Europe connait des difficultés. Plusieurs causes en sont à l'origine. La Commission européenne a ainsi établi un rapport le 15 mars 2006[196] constatant que la technologie de la clé publique et privée est complexe et coûteuse, ce qui entraine un ralentissement du marché de la signature électronique. De plus, la Commission souligne le manque d'opérabilité des systèmes transfrontaliers, au plan national et international. Elle propose donc de mettre en place des dispositifs de création et de vérification de la signature électronique dans les textes normatifs communautaires, même exiger la signature électronique.

181. Néanmoins, en l'état actuel, la Directive de 1999 sur la signature électronique assure entre les Etats membres de l'UE la libre fourniture de services de certification et la libre circulation des produits dans le marché communautaire. Cela signifie que les certificats des

[195] Dir. 1999/93/CE, 13 déc. 1999, préc.
[196] Commission, *Rapport sur la mise en œuvre de la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques*, Bruxelles, 15 mars 2006, COM/2006/0120 final

dispositifs sécurisés de création de signature électronique sont reconnus par les Etats membres si ces certificats sont issus d'un Etat membre[197].

B. La signature électronique en Allemagne

182. L'Allemagne a transposé la Directive de 1999 « *Sur un cadre communautaire pour les signatures électroniques* »[198] dans les délais par une Loi du 16 mai 2001.[199]

183. En ce qui concerne la définition de la signature électronique : la Loi allemande ne pose pas de définition juridique afin de rester ouverte sur d'éventuelles évolutions technologiques, même si en fin de compte elle prévoit un type précis de signature électronique, celui de la signature par cryptographie asymétrique.

184. Selon la définition allemande, la signature électronique se présente sous la forme de « *données sous forme électronique, accompagnant d'autres données électroniques ou qui peuvent leur être logiquement reliées et qui servent à l'authentification*. ». C'est pratiquement la définition donnée par la Directive de 1999 mais elle est très différente de la définition française qui précise que la signature électronique « *consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache*[200]. »

185. Selon la définition allemande, les prestataires de service sont des « personnes physiques ou morales qui produisent de certificats qualifiés ou des certificats d'horodatage qualifiés. ». La Directive de 1999 quant à elle vise « *toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques.*[201] ». On peut remarquer que le législateur allemand s'est plus focalisé sur l'accréditation des prestataires de service que le contrôle des produits de signature (contrôle en amont) tandis que le législateur français s'est, à l'inverse, plus focalisé sur le contrôle des produits de signature (contrôle en aval). La législation allemande est portée sur une sécurité maximale des produits

[197] Décr. n° 2001-272, 30 mars 2001, préc., art 3 II 2° et Décr. n° 2002-535, 18 avr. 2002, préc., art. 9, al. 2
[198] Dir. 1999/93/CE, 13 déc. 1999, préc.
[199] *GesetzüberRahmenbedingungenfürelektronischeSignaturen* (SigG), 16 mai 2001
[200] C. civ., art. 1316-4
[201] Dir. 1999/93/CE, 13 déc. 1999, préc., art. 2.11

de signature, par une accréditation sévère des prestataires de service, et donc une grande présence étatique.

186. On peut en conclure que la Directive de 1999 est « librement » transposée dans les Etats européens. Le cas de l'Allemagne montre que l'acception de la signature électronique n'est pas la même dans tous les Etats membres, sur la définition même de la signature électronique. Même si la Directive a le rôle d'harmoniser les règles en la matière, les difficultés subsistent en fonction du degré d'importance différent donné à la place de l'électronique par l'Etat.

187. La signature électronique n'a pas de place uniquement en Europe, elle se développe partout dans le Monde.

§ 2 L'état des lieux hors Union européenne

188. Il convient de noter que la signature se développe à l'échelle mondiale (A), et notamment aux Etats-Unis (B).

A. La signature électronique à l'échelle mondiale

189. Le **certificat électronique** délivré par un prestataire étranger a la même valeur que celui qui est établi par un prestataire européen, dès lors que le certificat a été garanti par un prestataire de l'Union européenne ou qu'un accord auquel l'Union est partie l'a prévu[202].En outre, la DCSSI et le COFRAC ont passé des accords de reconnaissance mutuelle avec des organismes étrangers et européens[203].

190. Pour ce qui est des **Etats-Unis**, un texte légalise la signature électronique à l'échelle fédérale des Etats-Unis, il s'agit de l'*E-Sign Act* du 30 juin 2000[204].

191. En **Chine**, une Loi du 1er avril 2005 permet d'identifier le signataire et de confirmer le contenu du document.

[202] Dir. 1999/93/CE, 13 déc. 1999, préc., art. 7
[203] Cf. http://www.cofrac.fr
[204] Electronic signatures in Global and National Commerce Act, 30 juin 2000, S. 761

192. L'**Egypte** a adopté une Loi en octobre 2009 instaurant un mécanisme de signature électronique dans le domaine commercial et administratif.

193. La **Tunisie**, quant à elle, a instauré la signature électronique pour les échanges commerciaux, par une Loi du 9 août 2000[205].

B. La signature électronique aux Etats-Unis

194. Aux Etats-Unis, une Loi a été votée le 30 juin 2000, « *Electronic Signatures in Global an National Commerce Act* » (appelée « *E-sign* »)[206] entrée en vigueur dans la majorité de ses dispositions le 1er octobre 2000. Elle a un but principal : l'harmonisation des règles étatiques sur la signature électronique aux Etats-Unis. De plus, la commission d'uniformisation des droits étatiques américains a adopté un acte : « *National Conference of Commissioners Electronic Transactions Act* » (appelée « *UETA* »)[207] adopté par moins de la moitié des Etats.

195. En France et aux Etats-Unis, la définition et le rôle de la signature électronique sont les mêmes. Elle vise à établir l'identité de son auteur, d'établir la légalité de l'acte concerné puis de manifester la volonté du signataire de consentir aux obligations contractuelles.

196. La **fraude** est une préoccupation majeure des Etats-Unis, dont leur législation tente de rendre la signature électronique plus fiable.

197. En France la procédure d'**identification** doit être respectée pour que la signature électronique soit valable. Aux Etats-Unis l'*E-Sign*et l'UETA sont muets sur ce point. *E-Sign* utilise la **certification par un tiers** (« *Notarization* »), un officier assermenté plus exactement (*notary*). Il utilise également la confirmation (« *Aknowledgment* »). La certification est alors dite « conforme ». Cependant elle peut être effectuée par voie électronique. La certification par un tiers en France des actes authentiques ressemble à celle des Etats-Unis mais peut-être effectuée par voie électronique sans la présence de l'officier assermenté.

[205] L. n° 2000-83, 9 août 2000, JO n°64, p. 1887

[206] *Electronic Signatures in Global and National Commerce Act*, Pub. L. No. 106-229, 114 Stat. 464 (1er octobre 2000) http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/content-detail.html

[207] The National Conference of Commissioners on Uniform State Laws, Uniform Electronic Transactions Act (23 au 30 juillet 1999), http://www.law.upenn.edu/bll/ulc/uecicta/uetast84.htm

198. On peut citer au moins **trois actions législatives aux Etats-Unis** :

-la création d'une administration par l'**Etat de New-York**: le Bureau de la Technologie (the « *Office for Technology* »[208]). L'Etat de New-York dispose en effet d'exigences propres en matière de signature électronique telles que stipulées dans l' « *Electronic Signatures and Records Act*[209] ». Son rôle est de déterminer si une technologie peut être utilisée dans un contexte informatique donné ;

-l'**Etat du Colorado** a adopté une législation spéciale également : il accepte des requêtes exercées par voie électronique dans les domaines du droit civil, droit de la famille, droit des successions et droit de la propriété[210] ;

-l'**Etat de Floride** quant à lui autorise l'exécution par voie électronique des emprunts hypothécaires[211].

199. On peut constater que la signature électronique détient une place dans le monde, plus ou moins importante selon les Etats. Elle connaît donc un succès indéniable, dû principalement à son efficacité. En effet, elle facilite les échanges, y compris économiques puisqu'elle est capable de traverser les frontières en dehors de tout contexte temporel et territorial. La magie de l'électronique s'opère dans n'importe quel pays et dans tous les domaines. La signature électronique est utile et efficace. La législation tente de diminuer autant que possible les risques de fraude, qui peuvent néanmoins subsister. Mais on a vu qu'elle se développe en France dans de nombreux domaines et continuera de se développer.

[208] Electronic Signatures and Records Act (ESRA), 9 N.Y.C.R.R. Part 540.3
[209] Electronic Signatures and Records Act (ESRA), 9 N.Y.C.R.R. Part 540 (2000), cf. infra
[210] Colorado Courts First in Nation to Offer Statewide E-Filing in Civil and Domestic Cases (7 août 2000), http://www.justicelink.com
[211] http://www.abanet.org

CONCLUSION

200. L'**introduction de la signature électronique** par la Loi du 13 mars 2000[212] et l'adaptation de la preuve électronique aux règles déjà établies avec la Loi du 21 juin 2004[213]bouleversent notre droit français. On peut considérer qu'il le bouleverse avec l'apparition de l'écrit électronique dans le droit français, et le fait évoluer avec l'adaptation des règles de l'acte support écrit à l'acte électronique. L'écrit électronique est désormais au cœur de la technologie et au cœur des relations contractuelles. La peur des contractants de la virtualité des échanges diminuent petit à petit face au développement des techniques de sécurisation et de fiabilité. Les utilisateurs d'internet veulent échanger électroniquement dans la sécurité. Pour répondre à ce besoin, l'utilisateur doit être en mesure de s'entourer de garanties techniques.

201. L'**identité** et la reconnaissance électronique des contractants est un phénomène en constante évolution. La signature électronique est un dispositif qui offre le choix de la simplicité mais non sans sécurité, avec la signature électronique simple, ou de la sécurisation avec une technicité non sans complexité mais avec une grande garantie d'authentification. Il ne faut pas oublier la présomption de responsabilité pesant sur les prestataires de services de certification électronique. La présence de tiers de confiance ajoute à la fiabilité de la signature électronique. « *La sécurité, c'est une garantie de confidentialité* (…)[214]».

202. L'écrit électronique et la signature électronique se développent dans de nombreux domaines dans les textes. Elle s'étend à un nombre de matières croissant et cette augmentation ne semble pas terminée. La technologie informatique, en constant progrès n'est pas sans effet sur la « technologie juridique » nouvellement acquise. En pratique, l'utilisation de la signature électronique connaît également un véritable succès. Les professionnels sont confrontés à une « réalité électronique » qu'ils ne peuvent ignorer. La sécurisation de la signature électronique leur est bien évidemment nécessaire pour conserver l'intégrité de leurs actes, la confidentialité également. La peur des risques de fraude diminue grâce au développement constant de techniques de sécurisation plus évoluées.

[212] L. n° 2000-230, 13 mars 2000, préc.
[213] L. n° 2004-575, 21 juin 2004, préc.
[214] T. PIETTE-COUDOL, *Echanges électroniques, Certification et sécurité*, préc., préface

203. L'**émergence de la biométrie** ajoute à ce progrès. Certains assimilent même la biométrie à un type de signature électronique puisqu'elle permet d'identifier une personne. Il n'est pas sans dire que toutes ces innovations facilitent les échanges, accélèrent les processus.

204. D'autres systèmes électroniques voient le jour. Nous avons connu l'**émergence de la Carte Vitale 2**, contenant la photo du propriétaire et la possibilité de combiner le remboursement des deux régimes de sécurité sociale et de mutuelle complémentaire en un seul support. La puce sert d'authentification, d'identification et de signature électronique. Elle servira peut-être de moyen pour l'assuré d'avoir accès à son dossier médical électronique ?

205. Le **domaine du droit de la santé** perce aussi en électronique : la dématérialisation des données de santé est au cœur de la modernisation des systèmes d'informations de santé. Depuis plusieurs années les échanges de données médicales sont faits de manière électronique, faisant appel à des messageries sécurisées pour garantir la sécurité et l'intégrité des données. Dans le cadre du plan Hôpital 2012, l'Etat a prévu de mettre en place des mesures mettant en première loge l'échange électronique : le Dossier médical personnalisé, le Dossier pharmaceutique, la Carte professionnelle de santé et le développement de la télémédecine qui avait déjà été créée en 2009[215].

206. Enfin, on assistera bientôt à la **carte d'identité électronique** qui sera une carte à puce d'un format identique à une carte bancaire ou une carte vitale. Elle pourra être lue par un lecteur de carte et sera un outil d'identification sécurisé. La CNIE[216]stockera un certificat émis par un certificateur qui sera accessible en lecture. Le processus utilisera une clef publique.

[215] L. n° 2009-879, 21 juill. 2009, portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, JO n°0167, 22 juill. 2009, p. 12184, t. n° 1 ;
http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020879475
[216] Carte nationale d'identité électronique

TABLE DES MATIERES

BIBLIOGRAPHIE

Manuels :

-C. FERAL-SCHUHL, *Cyberdroit : le droit à l'épreuve de l'internet*, 6ème éd., Dalloz, Coll. Praxis Dalloz, Paris 2010, p.686-708

-V. FAUCHOUX et P. DEPREZ, *Lois, contrats et usages*, LexisNexis, Coll. Litec, 2008, Paris, p. 116-117 ; p. 354-357

- PH. LE TOURNEAU, *Droit de la responsabilité et des contrats*, Coll. Dalloz Action, D., 8ème éd. févr. 2010, Paris, p. 912

-T. PIETTE-COUDOL, *Echanges électroniques, Certification et sécurité*, Coll. Maitriser, éd. Litec, Paris 2000, p. 15, §25

-E. RENAN, *L'avenir de la science*, Flammarion, 1995, p. 91

-R. SAVATIER, *Les métamorphoses économiques et sociales du droit privé aujourd'hui, seconde série. L'universalisme renouvelé des disciplines juridiques*, Dalloz, 1959, p. 49

Articles de doctrine :

-T. ABALLEA, *Signature électronique, quelle force pour la présomption légale ?*, D. 2004, p. 2235

-P. AGOSTI, *De la fiabilité d'un procédé de signature "électronique"*, JCP G. n° 41, 10 oct. 2001, II 10606, p. 2-5

-L. ASSAYA, *La signature électronique par cryptographie à clef publique*, JCP E. n° 4, 23 janv. 2003, 146, §14

-P. BALLET et A-L BENEAT, *Dématérialisation des données de santé : quels référentiels* , Gaz. Pal., 22 janv. 2011, n° 22, p. 22

-L. BIRNBAUM-SARCY et F. DARQUES-LANE, *La signature électronique comparaison entre les législations française et américaine, "Electronic signature comparison between french & U.S Law"*, RDAI/IBLJ, n° 5, 2001, p. 543-552

-A. BOBANT et N. DESSARD, *La signature électronique appliquée aux actes d'huissier*s, Gaz. Pal., 20 avr. 2006, n° 110, p. 22

-X. BUFFET DELMAS D'AUTANE, *L'achèvement du cadre juridique de la signature électronique sécurisée. Décret n° 2002-535 du 18 avril 2002 et Arrêté du 31 mai 2002*, JCP G. n° 49, 4 déc. 2002, act. 519, p. 1 et 3

-M. CABRILLAC, *Un effet de commerce peut-il être signé électroniquement ?*, RTD Com., 2001, p. 194

-E. A CAPRIOLI, *Sécurité et confiance dans le commerce électronique : signature numérique et autorité de certification*, JCP G., n° 14, 1er avr. 1998, I 123, p. 1, §1et §2; p. 2, §6 ;

-E. A. CAPRIOLI, *La signature électronique dans les communications par voie électronique en matière de procédure civile*, CCE, n° 7, juill. 2010, comm. 80, p. 2

- E. A CAPRIOLI, *Signature et confiance dans les communications électroniques en droit français et européen*, in Libre droit, Mélanges Ph. Le Tourneau : Dalloz, 2008, p. 55 et s.

-E. A. CAPRIOLI, *HADOPI et signature électronique des procès-verbaux des agents*, CCE, n° 10, oct. 2010, comm. 104, p. 1

-E.A CAPRIOLI, *Procédure pénale et signature numérique*, CCE, n° 10, oct. 2010, comm. 103, p. 1 et 2

-E. A CAPRIOLI, *Vérification d'écriture et courrier électronique*, CCE, n° 12, déc. 2010, comm. 129, p. 1-3

-E.A CAPRIOLI, *La lettre recommandée électronique, un nouveau décret pour la « confiance numérique* », CCE, n° 4, avr. 2011, comm. 40, p. 1-4

-P. CATALA, *L'introduction de la preuve électronique dans le code civil*, JCP G. n° 47, 24 nov. 1999, I 182, p. 4, §8

-P. CATALA, *L'engagement de l'entreprise*, Rev. soc., 2001, p. 258

-C. CATHIARD, *L'utilisation des moyens de télécommunication pour la préparation et la tenue des conseils et assemblées des sociétés anonymes*, JCP E., n° 20, 17 mai 2007, 1660, p. 4, §24

-L.CLUZEL-METAYER, *La signature électronique des actes des autorités administratives*, Dr. adm. n° 10, oct. 2010, prat. 4, p. 1 et 2

-L. DARGENT, *Nouvelles technologies et justice*, D., 30 oct. 2008

-N. DESSARD, *Les premières significations par voie électronique en matière civile devant la Cour de cassation*, Gaz. Pal., 23 avr. 2011, n° 113, p. 13

-C. DEVYS, *Du sceau numérique à la signature numérique*, Rapp. OJTI, nov.1995, pub.in OJTI, ss dir. C. -DHENIN, *Vers une administration sans papiers*, Paris, La documentation française, 1996, p. 96

-P-Y GAUTIER et X. LINANT de BELLEFONDS, *De l'écrit électronique et des signatures qui s'y attachent*, JCP G., n°24, 14 juin 2000, I 236, p. 1, §1

-P-Y GAUTIER, *Le bouleversement du droit de la preuve : vers un mode alternatif de conclusion des conventions*, PA n° 26, 7 févr. 2000, p. 4, §3 et §8

-L. GRYNBAUM, *La directive « commerce électronique » ou l'inquiétant retour de l'individualisme juridique*, JCP G., 21 mars 2001, I 307, p. 1-3, 6, 8-9

-L. GRYNBAUM, *Pour une bonne réception de la lettre recommandée électronique*, JCP E., n° 8, 24 fév. 2011, act. 98, p. 1-3

-B. JALUZOT, *Transposition de la Directive « signature électronique » : comparaison franco-allemande*, D. 2004, p. 2286

-V. LASSERRE-KIESOW, *Droit et technique*, JCP G., n° 4, 24 janv. 2011, 93, p. 1 et 2

-P. LECLERQ, *Propositions diverses d'évolutions législatives sur les signatures électroniques*, Dr. Informatique et télécoms, 1998, p. 19 s.

-F. LINDITCH, *Précisions sur la signature électronique*, Contrats marchés pub., n° 10, oct. 2010, alerte 50

-E. LOQUIN, *De l'usage de la télécopie pour signifier une sentence*, RTD Com., 2007, p. 686

-M-A LEDIEU, *Prestataires de certification électronique*, CCE, n° 10, oct. 2004, alerte 197, p. 1

-C. MALECKI, *Regards sur le formalisme cambiaire à l'heure de la signature électronique*, JCP E., n° 51, 21 déc. 2000, p. 2036, §1

-J. MARROCCHELLA, *Ecrit électronique : rappel de l'office du juge*, D. actu., 11 oct. 2010

-T. PIETTE-COUDOL, *La remise électronique du bulletin de paie*, JCP S., n° 43, 26 oct. 2010, 140, p. 2

-T. PIETTE-COUDOL, *LCEN. L'écrit électronique et la signature électronique depuis la LCEN*, CCE, n° 9, 9 sept. 2004, Etude 29, p. 1-3

-T. PIETTE-COUDOL, *Echanges électroniques, Certification et sécurité*, Coll. Maitriser, éd. Litec, Paris 2000, préface ; p. 15, §25

-T. PIETTE-COUDOL, *La remise électronique du bulletin de paie*, JCP S. n° 43, 26 oct. 2010, 1140, p. 2

-T. PIETTE-COUDOL, *Une signature électronique altérée vicie-t-elle la procédure dématérialisée ?*, CMP, n° 1, janv. 2011, comm. 5, p. 1-4

-T. PIETTE-COUDOL, *L'identité des personnes, les certificats et la signature électronique*, CCE, n° 1, janv. 2005, étude 2, p. 6-8

-J. RAYNARD, *Signature électronique, valeur probante, cryptologie et tiers certificateur*, RTD Civ., 2000, p. 449

-B. REYNIS, *La signature électronique notariale est reconnue sécurisée : une avancée majeure*, Defrénois, 30 oct. 2007, n° 20, p. 1411

-B. SAINTOURENS, *La réforme des conditions de délivrance par le greffier de copies, extraits ou certificats du RCS*, RTD Com., 2010, p. 59

-R. SERAICHE, *L'e-mail n'échappe pas aux exigences du Code civil pour bénéficier de la présomption de fiabilité reconnue aux écrits électroniques*, LPA, 3 janv. 2011, n° 1, p. 10

-S. STAUB, *Mode d'emploi pour une mise en place réussie de la signature électronique*, Option Finance, n° 701, 2 sept. 2002, p. 35

-M. STORCK, *Réglementation des contrats de services financiers à distance entre un professionnel et un consommateur*, RTD Com., 2005, p. 787

Textes officiels(en années):

Nationaux :

⇨ **1983 :**

-L. n° 83-1020, 30 avr. 1983, relative à la mise en harmonie des obligations comptables des commerçants et de certaines sociétés avec la IVè directive adoptée par le conseil des communautés européennes le 25 juillet 1978, JO 3 mai 1983

-D. n° 83-1020, 29 nov. 1983, pris en application de la loi n° 83-353 du 30 avril 1983 et relatif aux obligations comptables des commerçants, JO 1er déc. 1983, p. 3461

⇨ **1990 :**

-L. n° 90-1170, 29 déc. 1990, sur la réglementation des télécommunications, JO n°303, 30 déc. 1990, p. 16439

-L. n° 901168, 29 décembre 1990, de finances pour 1991, JO 30 déc. 1990

⇨ **1994 :**

-L. n° 94-126, 11 févr. 1994, relative à l'initiative et à l'entreprise individuelle, dite Loi Madelin, JO 13 févr. 1994, p. 2493

⇨ **1996 :**

-L. n° 96-659, 26 juill. 1996, de réglementation des télécommunications, JO n° 174, 27 juill. 1996, p. 11384

⇨ **1997 :**

-Conseil National du Crédit et du Titre, *« Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres »*, Mai 1997, Rapport p. 73 et 74

⇨ **1999 :**

-Décr. n° 99-200, 17 mars 1999, définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable, JO n° 66, 19 mars 1999, p. 4051

-L. n° 99-1173, 30 déc. 1999, de finances rectificative pour 1999, art. 41, insérant CGI, art. 1649 quater B quater et 1695 quater, JO n° 303, 31 déc. 1999, p. 19968

⇨ **2000 :**

-L. n° 2000-83, 9 août 2000, JO n°64, p. 1887

-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, JO n° 62, 14 mars 2000, p. 3968, t. n° 1

⇨ **2001 :**

-Décr. 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, p. 5070

⇨ **2002 :**

-Décr. n° 2002-535, 18 avr. 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 avr. 2002, p. 6944

-Arr. 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

-L. n° 2002-1576, 30 déc. 2002, de finances rectificative pour 2002, JO 31 déc. 2002, p. 22070

-Bull. COB, sept. 2002, n° 371, p. 119

⇨ **2003 :**

-Décr. n° 2003-632, 7 juill. 2003, relatif aux obligations de facturation en matière de taxe sur la valeur ajoutée et modifiant l'annexe II au code général des impôts et la deuxième partie du livre des procédures fiscales,JO 9 juill. 2003, p. 11617, t. n° 36

-Décr. n° 2003-659, 18 juill. 2003, relatif aux obligations de facturation en matière de taxe sur la valeur ajoutée et modifiant l'annexe III au code général des impôts et la deuxième partie du livre des procédures fiscales,JO 20 juill. 2003, p. 12272, t. n° 6

-Instr. Fisc. 7 août 2003, n° 136, BOI 3 C. A

⇨ **2004 :**

-L. n° 2004-575, 21 juin 2004, pour la confiance en l'économie numérique, dite LCEN, JO 22 juin 2004, p. 11168, t. n° 2

-Arr. n° 182, 26 juill. 2004, relatif à la reconnaissance de la qualification des prestataires de services de certification électronique, JO 7 août 2004, p. 14104, t. n° 17

⇨ **2005 :**

-Ord. n° 2005-674, 15 juin 2005, relative à l'accomplissement de certaines formalités contractuelles par voie électronique, JO 17 juin 2005, p. 10342, t. n° 26

-Ord. n° 2005-1516, 8 déc. 2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, par L. n° 2009-526, 12 mai 2009, de simplification et de clarification du droit et d'allègement des procédures, JO n° 0110, 13 mai 2009, p. 7920, t. n° 1

⇨ **2006 :**

-Décr. n° 2006-1566, 11 déc. 2006, modifiant le Décr. n° 67-236 du 23 mars 1967 sur les sociétés commerciales, JO 12 déc. 2006, p. 18762, t. n° 17

⇨ **2009 :**

-Décr. n° 2009-834, 7 juill. 2009, portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », JO n° 0156, 8 juill. 2009 , t. n° 3

-Circ., 20 juill. 2009, relative au changement de titulaire du marché, BO min. Justice, 30 oct. 2009, justice 2009/5, texte 1/29, p. 2

-Décr. n° 2009-1524, 9 déc. 2009, relatif à la procédure d'appel avec représentation obligatoire en matière civile, JO 11 déc. 2009, p. 21396, t. n° 8

-L. n° 2009-879, 21 juill. 2009, portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, JO n°0167, 22 juill. 2009, p. 12184, t. n° 1

⇨ **2010 :**

-Décr. n° 2010-434, 29 avril 2010, relatif à la communication par voie électronique en matière de procédure civile, JO 2 mai 2010, t. n° 17

⇨ **2011 :**

-Décr. n° 2011-144, 2 févr. 2011, relatif à l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat, JO n° 0029, 4 févr. 2011, p. 2274, t. n° 19

-Arr. 5 mai 2010, relatif à la communication par voie électronique dans les procédures sans représentation obligatoire devant les Cours d'appel, JO 15 mai 2010, p. 9041

-Décr. n° 2009-1150, 25 sept. 2009, relatif aux informations figurant sur les registre du commerce et des sociétés, JO 30 sept. 2009, p. 15840, t. n° 14

-Décr. n° 2010-671, 18 juin 2010, relatif à la signature électronique et numérique en matière pénale et modifiant certaines dispositions de droit pénal et de procédure pénale, JO 20 juin 2010, page 11183, t. n° 4

-L. n° 2009-526, 12 mai 2009, de simplification et de clarification du droit et d'allègement des procédures, JO n° 0110, 13 mai 2009, p.7920, t. n° 1

-Décr. n° 2005-972, 10 août 2005, modifiant le décret n° 56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice, JO 11 août 2005, p. 13095

-Décr. n° 2005-973, 10 août 2005, modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, JO 11 août 2005, p. 13095

-Arr. 17 juin 2008, portant application anticipée pour la procédure devant la Cour de cassation des dispositions relatives à la communication par voie électronique ; JO n° 0148, 26 juin 2008, p. 10259, t. n° 27

Européens:

-Commission, « *Rapport sur la mise en œuvre de la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques* », Bruxelles, 15 mars 2006, COM/2006/0120 final

-Dir. 1999/93/CE du Parlement et du Conseil, 13 déc. 1999, sur un cadre communautaire pour les signatures électroniques, JOCE L 13, 19 janv. 2000, p. 12

-Position commune 28 fév. 2000, CE n° 22/2000, JOCE n° L. 128, 8 mai 2000, p. 32 et s.

-Dir. n° 2000/31/CE, 8 juin 2000, « Commerce électronique », JO n° L 178, 17 juill. 2000, p. 0001-0016

-Directive 2000/31/CE du Parlement européen et du Conseil, 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»), JO n° L 178, 17 juill. 2000, p. 0001-0016

-Dir. 2001/115/CE du Conseil, 20 déc. 2001, JOCE L 015, 17 janv. 2002, p. 24

Internationaux :

-CNUDCI, note du Secrétariat, Doc. A/CN.9/WG.IV/WP.71, 31 déc. 1996, V. § 55.

-CNUDCI, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente et unième session, Doc. A/CN.9/437, 12 mars 1997

-L. type CNUDCI, 16 déc. 1996, sur le commerce électronique, A/RES/51/162

-Rapp. Comm. Nations Unies pour le droit commercial international sur les travaux de sa vingt-neuvième session, 28 mai-14 juin 1996, Assemblée générale, Documents officiels, Cinquante et unième session, suppl. n° 17 (A/51/17), V. p. 77

-*NYS Technology Law*, 28 septembre 1999

-*The National Conference of Commissioners on Uniform State Laws, Uniform Electronic Transactions Act* (23 au 30 juillet 1999)

-*Electronic Signatures in Global and National Commerce Act*, Pub. L. No. 106-229, 114 Stat. 464 (1er octobre 2000)

-*Electronic signatures in Global and National Commerce Act*, 30 juin 2000, S. 761

-*Electronic Signatures and Records Act (ESRA)*, 9 N.Y.C.R.R.,Part 540, 2000

-*GesetzüberRahmenbedingungenfürelektronischeSignaturen*(SigG), 16 mai 2001

-*Directives ISO/CEI*, part. 2, « Règles de structure et de rédaction des Normes internationales », 5ème éd., 2004, §3.1

Sites Internet:

www.legifrance.gouv.fr

www.uncitral.org

http://eur-lex.europa.eu

http://www.droitetjustice.org

www.dhimyotis.com

www.certeurope.fr

www.certigreffe.fr

www.ssi.gouv.fr

http://www.cofrac.fr

http://www.law.upenn.edu/bll/ulc/uecicta/uetast84.htm

http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/content-detail.html

http://www.justicelink.com

http://www.abanet.org

http://www.dictionnaire-juridique.com

Jurisprudences :

-CA Besançon, Ch. soc., 20 oct. 2000, SARL Chalets Boisson c/ Gros, JCP G. 2001, II, n° 10606, note E. A Caprioli

-Cass. com., 2 déc. 1997, JCP G. 1998, II, 10097, note Grynbaum; JCP E. 1998, n°5, p. 178, note T. Bonneau

-Cass. com., 15 déc. 1992, Bull. civ. IV, n° 419

-Civ. 1ère, 13 mars 2008, n°06-17.534, Bull. civ. I, n°73

-Cass. 1ère civ., 30 sept. 2010, n° 09-68.555, F-P+B+I, Michelet c/ Frachebois, JurisData n° 2010-017147

-Cass., crim., 27 mai 2008, n° 07-88.176, F-P+F, JurisData n° 2008-044294

-Cass. civ. 1ère, 30 sept. 2010, n° 09-68555, BICC n° 734, 15 janv. 2011

INDEX

A

B

C

D

E

F

G

I

M

P

Q

R

S

T