La nouvelle loi sur la signature électronique et le droit du bail

par Carole Aubert,

avocate, DEA en droit, criminalité et sécurité des nouvelles technologies

Sommaire

Page

I. Introduction 3

II. De la signature manuscrite à la signature électronique 3

1. Exigences de règles de forme 3

a) Principe et exceptions 3
b) Espèces de formes spéciales 5

2. La forme écrite et l'exigence de signature manuscrite 5

a) Généralités 5
b) Définition de la forme écrite simple 5
1. L'évolution nécessaire de la notion d'écrit 6
2. Le rôle et la notion de la signature 8
c) Autres formes écrites ? 8

3. La signature électronique 8

a) Introduction 8
b) Concept et exigences 8
c) Fonctionnement et explications techniques 10
1. Fonction de confidentialité 11
2. Fonction d'authentification / non-répudiation 11
3. Fonction d'intégrité 11
4. La signature numérique 12
5. Le rôle de l'autorité de certification 13

4. La loi fédérale sur les services de certification dans le domaine de la signature électronique 14

a) La genèse législative 14
b) Les différents types de signature électronique selon la SCSE 15
c) L'exigence de certificat qualifié 16
d) Le régime de responsabilité 17
1. Des fournisseurs de services de certification et des organismes de reconnaissance 17
2. Des titulaires d'une clé de signature (art. 59a CO nouveau) 17

e) Compatibilité avec le droit européen 18

5. Assimilation de la signature électronique qualifiée à la signature manuscrite 19

6. Problématique de la preuve numérique et de sa conservation 20

a) Principe 20
b) Production de la preuve numérique en justice 21
c) Fragilité et volatilité du support 22
d) Une solution ? La lettre recommandée électronique avec accusé de réception 23

III. Conséquences de l'introduction de la signature électronique en droit du bail 24

1. La conclusion du contrat de bail 24

a) Mécanisme de conclusion 24
b) Inclusion de conditions générales 27

2. Déclarations de volonté et exercice de droits formateurs 27

a) Titularité et exercice 27
b) Absence de forme particulière requise 28
c) Forme écrite requise 29
d) Le cas particulier de la formule officielle 29

3. Respect des termes et délais 30

IV. Conclusion 31

Bibliographie 32

Annexes :

- Loi fédérale sur les services de certification dans le domaine de la signature électronique
- Ordonnance sur les services de certification dans le domaine de la signature électronique

I. Introduction

Le recours de plus en plus fréquent à des techniques d'authentification électroniques en lieu et place de signatures manuscrites et d'autres méthodes traditionnelles d'authentification a conduit le législateur à définir un cadre juridique spécifique, afin de réduire l'incertitude quant à l'effet juridique pouvant résulter de l'utilisation de telles techniques modernes (qui peuvent être désignées d'une façon générale par le terme "signatures électroniques")[1].

Le commerce électronique n'a toutefois pas attendu une législation spécifique pour se développer avec succès[2]. Le législateur était cependant conscient qu'une adaptation législative était nécessaire, principalement afin de rassurer le consommateur et augmenter sa confiance.

Toutefois, mis à part la Loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique, SCSE) et ses textes d'exécution, aucune *législation spécifique* sur le commerce électronique n'a été adoptée en Suisse, contrairement à l'Union Européenne. C'est donc le droit ordinaire qui doit être interprété pour être adapté aux spécificités des relations juridiques sur le réseau.

Pour bien comprendre la notion de signature électronique, il convient dans un premier temps de reprendre la notion de signature en général et du rôle qui lui est assigné en droit privé, avant d'en venir à la signature électronique elle-même, puis enfin au rôle que celle-ci est amenée à jouer en droit du bail.

II. De la signature manuscrite à la signature électronique

1. Exigences de règles de forme

a) Principe et exceptions

Le droit privé repose sur le principe de l'autonomie privée. En droit des obligations, ce principe se concrétise dans celui de la liberté contractuelle. Cette liberté présente diverses facettes et notamment celle de la liberté de la forme[3].

Le régime du principe de liberté de la forme est prévu par l'art. 11 CO. Il suffit que chaque partie manifeste sa volonté d'une manière reconnaissable et compréhensible pour le destinataire ; le consentement est donc valable quelque soit la forme qu'il revêt. Toutes les formes d'expression de volonté doivent être prises en considération.

Par exception à ce principe, la validité de certains contrats (et d'autres actes juridiques) est subordonnée au respect d'une forme spéciale, qui peut avoir comme fondement la loi ou la volonté des parties. Le consentement est nécessaire mais insuffisant : il doit en plus revêtir une forme spéciale ("contrats formels" ou "formalistes").

---

1 Guide pour l'incorporation de la loi-type de la CNUDCI sur les signatures électroniques, New-York, 2001, p. 13.

2 La France a annoncé une croissance de l'e-commerce supérieure à 40% en 2004 et un chiffre d'affaires qui atteint les 7 milliards d'euros, selon une étude de Benchmark Group (www.benchmark.fr), mars 2006.

3 ATF 129 III 35, 42 = JT 2003 I, p. 127, 133.

Si l'ordre juridique ou la volonté des parties imposent un mode particulier à l'extériorisation d'une déclaration, l'acte juridique ne naît et ne vaut que si cette exigence a été respectée, car il s'agit d'une condition de validité de l'acte[4].

Dans la première hypothèse, c'est la loi qui impose le respect d'une forme spéciale. Ces règles ont alors un caractère impératif et les parties ne peuvent les exclure ou les alléger. L'exigence de forme entend principalement faire réfléchir les parties à leur engagement, protéger la partie la plus faible et assurer la sécurité des transactions[5].

Dans la seconde, ce sont les parties qui décident, par un accord préalable, que leur contrat ne sera conclu que si une forme spéciale est respectée (art. 16 CO). On parle alors de forme conventionnelle (ou réservée). Cette possibilité résulte de la liberté de la forme : les parties étant libres de contracter, sans l'exigence d'une forme spéciale, elle sont également libres de se lier au moyen d'une forme librement choisie et non impérativement prévue par le législateur.

Des partenaires peuvent donc s'engager valablement depuis longtemps par la voie électronique dans la mesure où ils respectent des procédures arrangées entre eux préalablement et que le contrat qu'ils entendent conclure n'est pas soumis légalement à une exigence de forme[6].

Il en va en particulier pour les principales transactions qui se déroulent aujourd'hui sur les réseaux informatiques, à savoir les ventes d'objets mobiliers[7], l'octroi de licences d'utilisation ou d'autres prestations de services en ligne.

En conséquence, le e-commerce s'est remarquablement développé ces dernières années et ce, sans législation particulière sur l'équivalence de la signature électronique avec la signature manuscrite.

La reconnaissance de la signature électronique en droit suisse tout comme en droit européen[8] s'inscrit dès lors beaucoup moins dans le cadre du formalisme que dans celui de la sécurisation des transactions commerciales en général, contrairement à d'autres pays[9]. Dans le monde traditionnel, la confiance placée dans la signature de son partenaire, permettant de l'identifier et attestant de son engagement, est fondamentale à la conduite du commerce et à la conclusion de

---

4 Engel, Traité des obligations en droit suisse, 2e éd., Berne 1997, p. 246.

5 Tercier, Le droit des obligations, 2e éd., 1999, p. 96 ; Guggenheim, Commentaire Romand, n° 2 ad art. 11 CO.

6 CdB 3/04, p. 94 (Jugement du Tribunal des Baux du canton de Vaud du 17 mars 2004), qui admet la validité d'une offre formulée par courrier électronique.

7 Par exemple, la société internationale eBay, propriétaire du site d'enchères éponyme, a annoncé un chiffre d'affaires mondial de plus de 4.55 milliards de dollars pour 2005 et plus de 168 millions d'utilisateurs inscrits.

8 En effet, l'objectif principal de la directive européenne n° 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques est de créer un cadre communautaire pour l'utilisation des signatures électroniques, de façon à permettre la libre circulation transfrontalière des produits et des services à signature électronique, et à assurer une reconnaissance juridique fondamentale des signatures électroniques. Il importe de souligner que la Directive ne porte pas sur la conclusion et la validité des contrats ni sur d'autres obligations légales imposées par le droit national ou le droit communautaire quant à la forme des contrats. Elle ne couvre pas non plus les règles et les restrictions relatives à l'utilisation des documents contenues dans le droit national ou le droit communautaire. Tous les vingt-cinq États membres de l'Union européenne ont désormais mis en oeuvre les grands principes de la directive (Rapport de la Commission au Parlement européen et au Conseil du 15 mars 2006 sur la mise en oeuvre de la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques, p. 4).

9 Jaccard, Le renforcement de la sécurité du droit par l'apport de la technologie: L'exemple de la signature électronique, DC 2002, p. 104.

contrats juridiquement contraignants[10]. Il convenait dès lors d'en trouver une équivalence dans le monde numérique afin de rassurer les utilisateurs et les consommateurs en particulier.

b) Espèces de formes spéciales

La forme écrite simple et la forme authentique sont les principales formes prévues par la loi. D'autres formes spéciales sont toutefois également réglementées, comme le testament olographe ou le pacte successoral, la légalisation, l'inscription dans un registre ou encore la mention dans les statuts [11].

2. La forme écrite et l'exigence de signature manuscrite

a) Généralités

La forme écrite est la seule qui soit réglementée en détail par le Code des Obligations. Celui-ci y consacre les art. 12 à 16 CO.

L'art. 13 CO dispose que « le contrat pour lequel la loi exige la forme écrite doit être signé par toutes les personnes auxquelles il impose des obligations ».

Dans certains cas, la loi exige en sus que le texte soit rédigé, en tout ou partie, à la main par son auteur (ex : testament olographe, art. 505 CC ; cautionnement, art. 493/2 CO). La forme écrite est alors dite « qualifiée », dans la mesure où il faut davantage que la seule signature de celui qui s'oblige. D'entente avec Guggenheim[12], nous estimons que n'appartiennent pas à cette dernière catégorie les cas où la loi prescrit expressément que certaines dispositions figurent par écrit dans le contrat (ex : art. 269d CO, art. 8 ss LCC).

b) Définition de la forme écrite simple

La forme écrite simple (appelée aussi "sous seing privé") suppose traditionnellement que le contenu de l'acte soit rédigé par écrit sur un support matériel et que celui qui s'engage ait authentifié le texte en y apposant sa signature (art. 13 à 15 CO). Cette forme comprend donc deux éléments : la notion *d'écrit* et la notion de *signature*.

Dans le cadre d'un exposé sur la signature électronique, il apparaît dès lors opportun de réinterpréter ces notions sous l'angle des nouvelles technologies.

On rappelle en effet que le Tribunal fédéral a jusqu'ici (et encore récemment) refusé d'assimiler le télex ou le téléfax à la forme écrite pour des motifs liés à l'absence de signature écrite originale[13].

---

10 Jaccard, Le renforcement de la sécurité du droit par l'apport de la technologie: L'exemple de la signature électronique, DC 2002, p. 99.

11 Engel, Traité des obligations en droit suisse, 2e éd., Berne 1997, p. 247 s.

12 Guggenheim, Commentaire Romand, n° 16 ad art. 13 CO: il s'agit d'éléments relatifs à la validité du contrat, au sens de clauses que le législateur considère comme essentielles.

13 ATF 112 II 326 = JT 1987 I 6; ATF 121 II 252 cons. 4a = JT 1997 I 188; confirmé in ATF 2A.546/2001 du 1er mai 2002.

Toutefois, avec l'avènement de la signature électronique la position de notre Haute Cour pourrait changer.

1. L'évolution nécessaire de la notion d'écrit

Si la portée des art. 12 à 15 CO sur la forme écrite s'étend à l'ensemble des actes juridiques[14], la notion « d'écrit » n'est pas elle-même définie par la loi. La doctrine retient en général que l'écrit est « un signe intelligible ou un ensemble de signes intelligibles sur un support matériel quelconque »[15].

Les contrats écrits appartiennent à la catégorie de titres relatifs à l'existence d'un droit[16]. Bien que la notion classique du titre en droit privé soit celle de l'« écrit manifestant une idée de son auteur », la notion *d'objet écrit* s'est relativisée, le support pouvant être tout objet matériel propre à recevoir une inscription. La doctrine récente admet ainsi que les supports impliquant l'emploi d'un moyen technique externe peuvent être compris parmi les titres[17].

La notion d'écrit est donc remplacée par la notion plus large d'agent d'information, qui a pour propriété de susciter chez celui qui le perçoit la représentation d'une idée autre que l'objet lui-même[18]. L'information véhiculée par le support se constitue dès lors "d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quelque soit leur support et leur modalité de transmission"[19].

La notion autrefois réservée à l'écrit s'élargit progressivement également dans d'autres domaines du droit[20].

Le support doit dès lors être apte à recevoir l'information, sa matière étant pour le reste indifférente. Le caractère aisément modifiable de l'information en particulier n'est pas un critère

---

14 ATF 101 III 65 = JT 1977 II 22 ; Guggenheim, Commentaire Romand, n° 2 ad 13 CO.

15 Engel, Traité des obligations en droit suisse, 2e éd., Berne 1997, p. 248 s.

16 Bohnet, La Théorie générale des papiers-valeurs, Thèse, Neuchâtel 2000, p. 101.

17 Rihm, E-Mail als Beweismittel im Zivilgerichtsverfahren, RSJ 96 (2000), p. 498-499; Bohnet, La Théorie générale des papiers-valeurs, Thèse, Neuchâtel 2000, p. 98 et note 689.

18 Bohnet, La Théorie générale des papiers-valeurs, Thèse, p. 98 et réf. citée ; Fanger, Digitale Dokumente als Beweis im Zivilprozess, Bâle 2005, p .124 et réf. citées à la note 861.

19 Définition de l'art. 1316 CCFR.

20 Le législateur fédéral a étendu la définition légale du titre de l'art. 110 ch. 5 CPS aux données mémorisées sur des supports de données ou d'images (par exemple : cd-rom, carte mémoire, etc.) pour mettre fin à une controverse. Les supports qui ne donnaient accès à l'inscription qu'à l'aide d'auxiliaires techniques (bandes magnétiques, disquettes, disques optiques, etc.) étaient admissibles dans certains cas, notamment lorsque la déclaration ne devait pas nécessairement être signée de manière manuscrite (ex : comptabilité commerciale ; ATF 111 IV 119). Le Tribunal fédéral avait ensuite précisé que ce n'étaient pas les données enregistrées sur un support magnétique au moyen d'un ordinateur comme telles, mais leur reproduction sous forme d'imprimé ou d'image sur écran (output), qui pouvaient être considérées comme des écrits ou signes et qui, par conséquent, pouvaient constituer un titre (ATF 116 IV 343 = JT 1992 IV 111).

La correspondance et les pièces comptables peuvent désormais être conservées sous forme électronique (art. 962 al. 2 CO). Depuis l'entrée en vigueur en 2002 des dispositions sur la comptabilité commerciale, cette règle vaut aussi pour la conservation des livres. Ces documents électroniques ont la même valeur probante que ceux qui sont lisibles directement (art. 957 al. 4 CO).

valable pour refuser la qualification de titre et donc d'écrit ; par contre, cela influencera sa valeur probante[21].

D'entente avec Guggenheim[22] , nous estimons dès lors que la qualification d'écrit ne doit pas être refusée à de l'information stockée sous format électronique, en raison notamment des risques de manipulation. En effet, l'écrit traditionnel ne donne nullement une garantie d'authenticité absolue, les risques de manipulation et d'usurpation étant tout aussi importants, voire supérieurs[23].

Même les titres sur papier n'emportent jamais de *présomption* d'authenticité (sauf les titres authentiques, cf. art. 9 CC) et n'offrent aucune *garantie* d'authenticité ; il ne faut dès lors pas se laisser aveugler par la technique. Si l'authenticité est contestée, il appartient à la partie qui se prévaut du titre de la prouver.

D'autre part, le droit pénal assimilant désormais à la notion de titre les données mémorisées sur des supports de données ou d'images, la personne qui manipulerait un document électronique répondant à cette nouvelle définition pourrait se rendre coupable de faux dans les titres, au sens de l'art. 251 CPS[24]. Cette disposition vient ainsi renforcer la valeur probante accordée aux titres numériques.

De même, l'avant-projet de Loi fédérale de procédure civile assimile tous les supports de données modernes à la notion de titre[25-26].

A notre avis, cette évolution est encore renforcée par l'introduction de la signature électronique : en effet, jusqu'ici, la forme écrite se satisfaisait de n'importe quel support et de n'importe quel écrit, pourvu qu'il fusse signé à la main. Désormais, du fait que la signature manuscrite n'est plus obligatoirement nécessaire, l'exigence de support matériel physique au sens traditionnel paraît d'autant moins nécessaire.

---

21 Bohnet, La Théorie générale des papiers-valeurs, Thèse, p. 98 note 689 et réf. citées ; Schlauri, Elektronische Signaturen, thèse, Zurich 2002, p. 169, n° 636 ; Aubert, La preuve numérique et son appréciation en procédure pénale et civile, Lausanne 2005.

L'art. 1316 du CCFr (modifié par la Loi nº 2000-230 du 13 mars 2000) dispose que « la preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission ». On voit ainsi que les lois modernes s'adaptent à une notion élargie de l'écrit.

22 Guggenheim, Commentaire Romand, n° 4 ad 13 CO et réf. citées.

23 Par exemple, on ne refusera pas la qualification d'écrit à un texte écrit au crayon de papier, aisément modifiable à l'aide d'une simple gomme.

24 ATF 119 IV 234 : l'amélioration de preuves dont on dispose dans le cadre d'un procès par la création d'un document tombe sous le coup de l'art. 251 CPS ; Donzallaz, La notification en droit interne suisse : étude de procédures civile, pénale et administrative cantonales et fédérales, Berne 2002, p. 332, n° 625.

25 Fanger, Digitale Dokumente als Beweis im Zivilprozess, Bâle 2005, p .116 et note 820.

26 « La notion de titres a été délibérément conçue de manière large pour faire face à la rapidité de l'évolution technologique. La présente disposition contient une énumération exemplative des documents qui entrent dans la notion de titres. La caractéristique de ces documents consiste en ce qu'ils doivent être propres à prouver des faits pertinents », Rapport accompagnant l'avant-projet de la commission d'experts, OFJ ; Juin 2003, p. 85.

2. Le rôle et la notion de la signature

L'exigence de signature a pour but *d'identifier* la personne qui s'oblige et constater qu'elle *reconnaît le contenu de sa déclaration*[27].

La signature doit en principe prendre en compte l'acte, soit établir l'appropriation du contenu de l'acte par l'auteur de la signature. Dès lors, la signature est traditionnellement apposée au bas du texte, sans être un principe absolu.

L'essentiel est que la relation entre la signature et le texte révèle sans aucun doute l'appropriation de toute la déclaration par quiconque veut en être l'auteur.

Dans la mesure où la signature remplit ce but, peu importe que le signataire utilise son nom de famille, son prénom ou un pseudonyme[28].

Jusqu'ici l'art. 14 CO imposait l'exigence d'une signature écrite de la propre main de celui qui s'obligeait. Des exceptions étaient prévues dans certains cas spéciaux (signature des aveugles, signature des personnes qui ne pouvaient pas signer et signature mécanique dans les affaires[29]).

En conséquence, et jusqu'à la modification récente de l'art. 14 CO par l'introduction d'un nouvel alinéa 2bis, aucun acte juridique que la loi soumettait à la forme écrite ne pouvait être valablement conclu en recourant à la signature électronique.

c) Autres formes écrites ?

Des dispositions législatives récentes *assimilent* certaines formes jugées *équivalentes* à la forme écrite du Code des obligations, pour autant que le moyen utilisé permette d'établir la preuve de la clause par un texte, notamment le télex, la télécopie ou la messagerie électronique[30].

3. La signature électronique

a) Introduction

L'information constitue la matière première de l'informatique et sa raison d'être. C'est sur elle que portent les traitements effectués par ordinateur. En effet, ce dernier permet de traiter, créer, transformer, stocker et communiquer l'information[31]. Pour pouvoir être traitée par un ordinateur,

---

27 ATF 119 III 6 = JT 1995 II 98.

28 Engel, Traité des obligations en droit suisse, 2e éd., Berne 1997, p. 252.

29 Art. 14 al. 2 et 3 CO et 15 CO.

30 Cf. art. 5 et 178 LDIP, art. 9 LFors. La validité des clauses d'élection de for n'est pas soumise à une forme particulière ; un échange de courriers électroniques non signés est donc suffisant. En revanche, les clauses d'arbitrage exigent d'être passées en la forme écrite si les deux parties sont domiciliées en Suisse. Si une des parties est domiciliée à l'étranger, aucune exigence de forme n'est imposée ; toutefois, étant entendu que la convention de New-York de 1958 pour la reconnaissance et l'exécution des sentences arbitrales étrangères exige une clause compromissoire écrite, la prudence exigera de continuer de passer de telles clauses par écrit et à l'aide d'une signature manuscrite. En effet, la convention délègue aux droits nationaux de déterminer la notion de la forme écrite. De nombreux droits n'ont pas encore élevé la signature électronique au même rang que la signature manuscrite.

31 Ghernaouti-Hélie/Dufour, De l'Ordinateur à la société de l'information, Que-Sais-Je n° 3541, 2e éd., PUF, Paris, 2001, p. 16 ss.

l'information doit être codée de façon numérique (ou digitale). Pour cela on lui fait subir une transformation dite de codage[32], qui s'appuie sur le langage binaire[33].

La numérisation de l'information implique dès lors sa dématérialisation, c'est-à-dire la dissociation de l'information et de son support. Le double numérique de l'information peut dès lors être sauvegardé, transmis et dupliqué de façon infinie. Quelle que soit sa nature (voix, données, image, multimédia), toute information est numérisable et possède une représentation homogène, c'est-à-dire uniforme.

La numérisation a dès lors pour effet de supprimer le support papier des informations traitées : on a recours à leur enregistrement sur ordinateur en détruisant éventuellement les originaux, ce qui constitue un avantage considérable en matière de gestion pour la rapidité des procédures, les facilités de classement et l'économie des coûts d'archivage. Mais cela représente un inconvénient de premier ordre : il devient difficile d'apporter la preuve d'un fait ou d'un acte selon les méthodes traditionnelles de preuve, c'est-à-dire notamment par la présentation d'un document écrit et signé[34].

Le concept de signature électronique a dès lors été développé dans l'optique de **renforcer la valeur probante** du document numérique.

b) Concept et exigences

Dans un premier temps, il convient de définir « techniquement » la notion de signature électronique au sens large et les différentes réalités qu'elle peut recouvrir. Toutefois, seule la *signature électronique qualifiée* est assimilée à la signature manuscrite par l'ordre juridique suisse ; elle doit répondre à des exigences précises définies par la loi, que nous examinerons plus bas (infra ch. II.4). Tout autre type de signature électronique au sens large n'est pas assimilé à la signature manuscrite et ne constituera qu'un indice parmi d'autres en cas de litige.

Lors de la réalisation d'un échange de consentements dématérialisé, certaines garanties de sécurité doivent être assurées pour que la signature électronique assure les mêmes fonctions que la signature manuscrite :

- L'authentification de l'auteur de l'acte ;
- L'intégrité du message (il ne doit pas avoir été altéré pendant son transport) ;

En outre, il doit être possible d'assurer :

- La confidentialité du message (il ne doit être compréhensible que par son destinataire, comme une lettre mise sous enveloppe dans le courrier postal),

---

32 La transformation d'un signal analogique en signal numérique est appelée **numérisation**. La numérisation comporte deux activités parallèles : l'**échantillonnage** (en anglais *sampling*) et la **quantification**. L'échantillonnage consiste à prélever périodiquement des échantillons d'un signal analogique. La quantification consiste à affecter une valeur numérique à chaque échantillon prélevé (http://www.commentcamarche.net/format/analog.php3).

33 Ce choix résulte de la physique des matériaux (allumé/éteint, ouvert/fermé). Un chiffre binaire (= un bit) constitue la plus petite unité d'information et ne peut donc revêtir que les valeurs 0 ou 1. Les caractères sont en principes codés sur une suite de 8 bits, que l'on nomme un octet (ou byte, en anglais).

34 **Linant de Bellefonds**, La pratique du droit de l'informatique, Paris, 2002, p. 301.

- La non-répudiation de l'acte (afin d'éviter une remise en cause du contenu du message par son auteur).

Plusieurs techniques d'authentification (signature électronique *au sens large*) peuvent être envisagées pour pallier la signature manuscrite dans le monde numérique :

- signature manuscrite numérisée (scanner) ;
- carte à puce (code PIN) ;
- procédés biométriques ;
- cryptage à l'aide de clés mathématiques.

Seul ce dernier système est aujourd'hui considéré comme offrant les meilleures garanties de sécurité. La signature numérique[35] recourt à une technique couplée de clé publique et de clé privée, par un mécanisme de cryptographie asymétrique qui requiert l'intervention d'un tiers de confiance, le fournisseur de services de certification numérique (cf. infra II.3.c.5).

Les autres techniques citées ont l'inconvénient de ne pas résoudre de manière satisfaisante les exigences d'intégrité et de confidentialité ou sont trop compliquées à mettre en œuvre (procédés biométriques par exemple), voire peu fiables. D'autre part, l'information présentée comme secrète doit en fait être connue de tous les partenaires à la transaction, entre qui elle doit être préalablement échangée, avec risque de fraude à la clé (ex : code PIN).

La signature électronique (ou numérique) *au sens étroit* peut être définie comme étant un procédé technique qui permet de déterminer l'origine d'un document électronique (authenticité), de s'assurer que le document n'a pas été modifié ultérieurement à la signature (intégrité). Comme elle permet de crypter les informations pour les protéger (confidentialité), outre sa fonction première d'authentification, la signature électronique au sens étroit introduit un élément de sécurité supplémentaire par rapport à la signature manuscrite.

c) Fonctionnement et explications techniques

Comme seules les signatures électroniques mettant en œuvre la cryptographie asymétrique (ou «à clé publique») permettent de garantir l'origine, l'intégrité et la confidentialité des communications avec un degré de fiabilité très élevé, c'est ce mode de cryptographie[36] qui est aujourd'hui employé pour le processus de signature électronique.

La signature électronique d'un fichier (texte, son, image) résulte de l'utilisation d'une clé mathématique privée (connue du seul signataire) et d'un algorithme cryptographique, appliqué au message original. Ainsi, la signature électronique constitue un ensemble de données

35 Si la signature électronique est le terme générique pour tout procédé d'identification autre qu'une marque manuscrite, les appellations « signature numérique » ou « signature digitale » sont en principes réservés aux procédés de signature à l'aide de la cryptographie asymétrique, Jaccard, Le renforcement de la sécurité du droit par l'apport de la technologie: L'exemple de la signature électronique, in : DC 2002, p. 101.

36 La cryptographie est l'art de transformer des informations lisibles (texte) en des informations que seules les personnes autorisées peuvent lire. Au cours de ce processus, l'information est codée (chiffrée) de façon à ce que seul le destinataire puisse lire ou altérer le message. Il peut être intercepté mais n'est intelligible que pour la personne qui est capable de le décoder (déchiffrer).

numériques chiffrées, distinctes du message original. Le lien entre le texte et sa signature n'est donc plus physique, mais *logique*.

Dans un système de cryptographie asymétrique, deux clés sont nécessaires pour que les deux parties puissent échanger des données de façon sûre[37] : une clé publique et une clé privée. L'une est utilisée pour chiffrer le message et seule l'autre clé de la paire permet de le déchiffrer. Cela fonctionne comme un cadenas avec une clé : on distribue le cadenas, toute le monde peut fermer le coffre avec le cadenas, mais seul le titulaire de la clé du cadenas peut ouvrir le coffre[38].

Bien que les deux clés de la paire soient liées de façon mathématique, il est impossible de trouver une clé à partir de l'autre. La clé privée ne peut donc être reproduite ou falsifiée à partir de la clé publique correspondante. Il est donc possible de distribuer sa clé publique, mais il est essentiel de garder sa clé privée *secrète*. Ainsi, à la différence du cryptage symétrique à clé secrète, celui à clé publique permet d'une part l'échange de la clé publique par l'intermédiaire d'un réseau ouvert non sécurisé et d'autre part, ne nécessite qu'une seule paire de clés[39].

L'utilisation combinée des quatre clés (clés publique/privée de l'expéditeur et clés publique/privée du destinataire) permet de garantir les propriétés attendues de la signature électronique :

- la clé publique de l'expéditeur est utilisée par le destinataire pour vérifier un message signé avec la clé privée de l'expéditeur (intégrité, authenticité, non répudiation) ;
- la clé publique du destinataire est utilisée par l'expéditeur pour chiffrer des messages qui ne pourront être déchiffrés que par le destinataire à l'aide de sa clé privée (confidentialité).

1. Fonction de confidentialité

Alice veut envoyer un message confidentiel à Bob. Alice va utiliser la clé publique de Bob pour sécuriser le texte. Bob sera donc le seul en mesure d'ouvrir le message envoyé par Alice, grâce à sa clé privée.

2. Fonction d'authentification / non-répudiation

Si Alice veut assurer à Bob que c'est bien elle qui a envoyé le message, elle va en revanche chiffrer le message avec sa clé privée ; pour le déchiffrer, Bob utilisera la clé publique d'Alice. Bob sera ainsi assuré que c'est bien Alice qui lui a envoyé le message, mais sa confidentialité n'est toutefois pas assurée (la clé publique d'Alice étant largement distribuée).

3. Fonction d'intégrité

Alice et Bob veulent s'assurer que les données du message envoyé par Alice ne seront pas modifiées lors de la transmission et veulent pouvoir ainsi détecter les modifications qui seraient éventuellement introduites par un tiers.

---

37 Contrairement au système à clé secrète (ou cryptographie symétrique), qui permet de chiffrer et de déchiffrer le contenu d'un message à l'aide d'une clé unique. L'inconvénient majeur de ce système réside dans sa vulnérabilité aux tentatives d'interception lors de la transmission de la clé et d'autre part nécessite autant de clés que de partenaires.

38 Jaccard, Le renforcement de la sécurité du droit par l'apport de la technologie: L'exemple de la signature électronique DC 2002, p.100 ss ; voir aussi www.commentcamarche.net/crypto/clepublique.php3.

39 Donzallaz, La notification en droit interne suisse : étude de procédures civile, pénale et administrative cantonales et fédérales, p. 320, n° 601 et note 1208.

Alice utilise à cette fin une *fonction de hachage*, qui transforme le message, de taille variable, en un condensé (*hash*, empreinte, résumé ou *digest*) de taille fixe qui est la signature unique du message d'origine (sorte « d'empreinte digitale » du message). Aucun autre message ne peut aboutir au même résumé. Cela signifie que si quelqu'un modifie le message d'origine, le résumé de la fonction de hachage ne sera pas identique et l'on s'apercevra de l'altération du message. La fonction doit être à sens unique (*one-way function*) afin qu'il soit impossible de retrouver le message original à partir du condensé. Alice va ensuite utiliser sa clé privée pour chiffrer cette empreinte et l'envoyer à son destinataire avec le message ; Bob déchiffrera le condensé à l'aide de la clé publique d'Alice et le comparera avec son propre résumé (schéma 1).

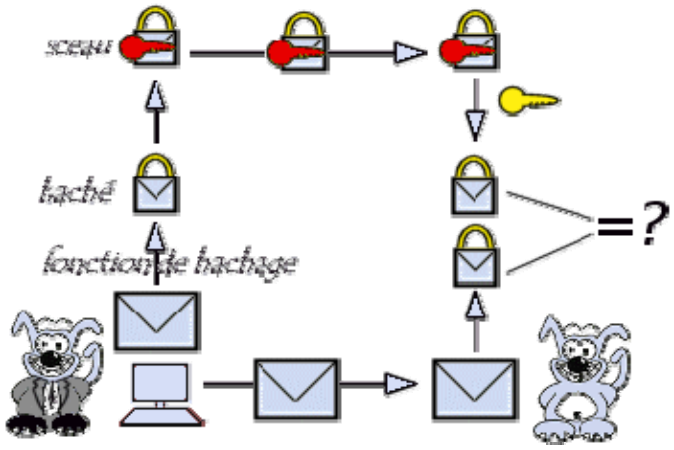

schéma 1(source: www.commentcamarche.net)

4. La signature numérique

Pour créer une signature numérique, le signataire va créer un résumé (digest) du message, qu'il cryptera avec sa clé privée et communiquera au destinataire en même temps que le message d'origine. Le destinataire va utiliser la clé publique de l'expéditeur pour déchiffrer la signature numérique et la comparer au résultat du hash obtenu du message original (schéma 2). S'ils correspondent, c'est la garantie que :

- le message a été signé électroniquement par le titulaire de la clé privée correspondante. *L'authentification* du signataire est vérifiée. La signature numérique assure également une fonction de *non-répudiation*, car elle empêche l'expéditeur de nier avoir expédié le message ;
- L'*intégrité* du message est vérifiée, le message n'a pas été modifié ni altéré pendant sa transmission, puisque seul le titulaire de la clé privée peut générer une signature numérique et qu'il est (quasiment) impossible de la reconstituer en connaissant uniquement la clé publique.

La *confidentialité* de la transmission est par ailleurs assurée si l'expéditeur du message le chiffre avec la clé publique du destinataire avant de le signer électroniquement avec sa propre clé privée. Dans ce cas, l'empreinte (*hash*) sera alors calculée à partir du message préalablement chiffré.

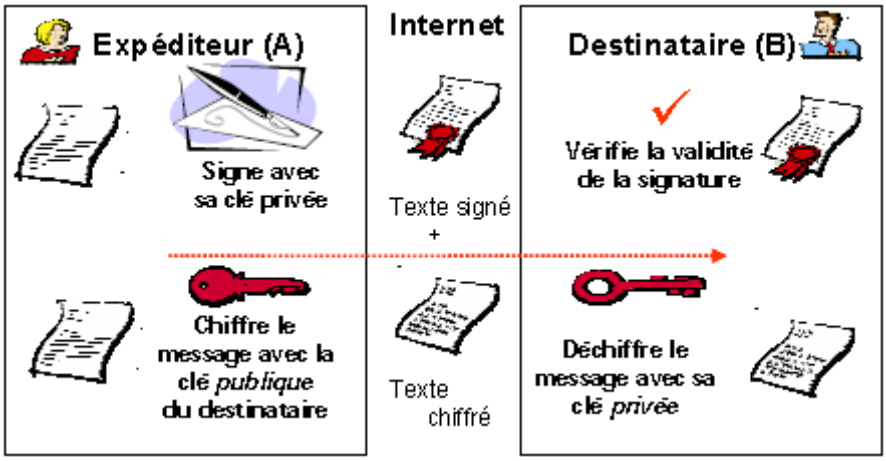

schéma 2 (source : La Poste Suisse)

5. Le rôle de l'autorité de certification

Une paire de clés (clé publique + clé privée) n'est pas vraiment associée à une identité, car il ne s'agit que d'une paire de chiffres. D'autre part, contrairement à la signature manuscrite, unique et invariable vu son lien intime avec son auteur, la signature numérique se modifie en fonction du message à signer et ne contient aucune marque individuelle susceptible d'identifier son auteur et la clé privée du signataire. En ce sens, c'est plutôt la clé privée qui se rapproche de la signature manuscrite[40]. Une signature numérique ne peut dès lors être reliée à une entité de façon non ambiguë que si un document certifié par une autorité de confiance atteste du **lien** entre la clé publique de l'entité et son identité.

Pour garantir que la clé est bien celle de l'utilisateur à qui elle est associée, on fait appel à des **certificats**[41]. Le certificat est en quelque sorte la carte d'identité de la paire de clés asymétriques, délivré par un organisme appelé **autorité de certification** (souvent notée CA pour Certification Authority). L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (sorte de date limite de péremption), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire). Outre la mise à jour du registre contenant les certificats qu'elle a émis, l'autorité doit prendre soin de permettre sa consultation à tout moment.

Les relations qui s'établissent entre l'autorité de certification, les titulaires de certificats et ceux qui s'y fient forment une *infrastructure à clé publique* (= PKI, Public Key Infrastructure) (schéma 3) :

40 Jaccard, Forme, preuve et signature électronique, p. 121, in Aspects juridiques du commerce électronique, Zurich 2001.

41 Le certificat électronique (ou certificat numérique) se présente sous la forme d'un bloc de données contenant, dans un format spécifié, les parties suivantes (http://www.commentcamarche.net/crypto/certificat.php3) (cf. art. 7 SCSE) :

- la partie publique d'une paire de clés asymétriques,
- des informations sur le porteur de cette paire de clés, telles que son nom, son adresse électronique, son numéro de téléphone, le nom de l'entité qui a délivrée ce certificat, la durée de validité du certificat, etc.
- la signature numérique des données ci-dessus par l'entité prenant en charge la création de ce certificat et ayant autorité de certification.

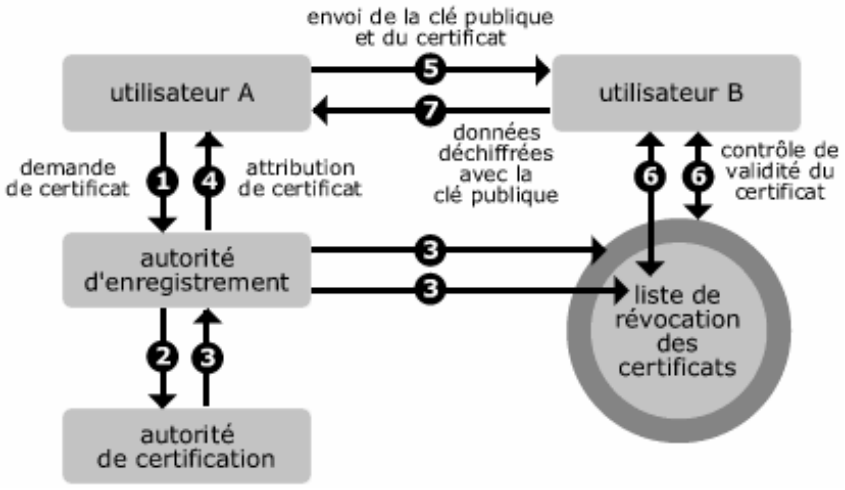

Schéma 3 (source : autorité wallonne des télécommunications)

Une signature électronique n'est donc « sûre » que dans la mesure où elle est certifiée de manière fiable. L'Etat fixe donc les règles auxquelles doit se soumettre un fournisseur de services de certification pour être reconnu. C'est donc la définition de la **qualité** des certificats et son contrôle par l'Etat qui vont créer la confiance dans la signature électronique[42].

4. La loi fédérale sur les services de certification dans le domaine de la signature électronique

a) La genèse législative

Afin de promouvoir l'utilisation et la reconnaissance juridique de la signature électronique, le Conseil fédéral a arrêté en 2000 des dispositions permettant aux fournisseurs de services de certification de se faire reconnaître sur une base volontaire (ordonnance du 12 avril 2000 sur les services de certification électronique, OSCert). Cette ordonnance, contrairement à la directive 1999/93/CE, ne consacrait pas l'équivalence entre signature électronique et signature manuscrite. Le Conseil fédéral était toutefois conscient que l'ordonnance était surtout destinée à établir un cadre réglementaire provisoire, dans l'attente d'une loi fédérale qui réglementerait d'une manière plus complète la question[43].

Adoptée par le Parlement le 19 décembre 2003, la loi fédérale sur les services de certification dans le domaine de la signature électronique (loi sur la signature électronique, SCSE) est entrée en vigueur le 1er janvier 2005, en même temps que l'ordonnance sur les services de certification dans le domaine de la signature électronique (ordonnance sur la signature électronique, OSCSE) adoptée par le Conseil fédéral.

---

42 Dans le cadre de projets d'e-government, certains Etats (ex : Belgique) ont décidé de doter leurs citoyens de cartes d'identité électroniques, contenant leur propre signature électronique (basée notamment sur des procédés biométriques). Dès lors, les citoyens pourront s'authentifier et signer des documents électroniques à l'aide d'une signature électronique unique qui sera reconnue par les entreprises, les citoyens et les autorités. Cette proposition a provoqué de vifs débats en France (http://www.foruminternet.org/carte_identite/). En Suisse, le Conseil fédéral a chargé le DFJP en 2002 d'élaborer un concept et un projet de loi (http://www.ejpd.admin.ch/ejpd/fr/home/dokumentation/mi/2002/2002-07-030.html).

43 Jaccard, Le renforcement de la sécurité du droit par l'apport de la technologie: L'exemple de la signature électronique, DC 2002, p. 104.

La SCSE définit les conditions qu'une signature électronique doit satisfaire pour être assimilée à une signature manuscrite et règle la question de la responsabilité des fournisseurs de services de certification, des organismes de reconnaissance et des titulaires de clés de signature. Elle définit en outre les conditions auxquelles les fournisseurs de services de certification peuvent être reconnus sur une base volontaire et règle leurs activités dans le domaine des certificats électroniques.

L'OSCSE a abrogé formellement le régime expérimental instauré par le Conseil fédéral en 2000. Elle concrétise en particulier les obligations auxquelles les fournisseurs de services de certification sont soumis une fois reconnus et charge l'OFCOM d'édicter les prescriptions techniques et administratives nécessaires.

Bien qu'elle se concentre essentiellement sur des questions de commerce électronique (e-commerce), la SCSE crée également la base légale des relations électroniques avec les autorités (*e-government*), permettant de communiquer avec les registres du droit fédéral (Registre fédéral du commerce, Registre foncier, etc.) ou d'autres autorités[44] une fois les dispositions d'exécution nécessaires adoptées[45]. Le Conseil fédéral a notamment décidé une révision complète de l'ordonnance sur la Feuille officielle suisse du commerce (FOSC). L'ordonnance révisée est entrée en vigueur le 1er mars 2006 et permet, pour la première fois, l'emploi d'une signature numérique qualifiée pour la publication de données économiques de portée juridique sur Internet[46].

b) Les différents types de signature électronique selon la SCSE

L'art. 2 SCSE définit les différents degrés de signature électronique[47]. Il distingue entre signature électronique simple, avancée et qualifiée, mais seule cette dernière est assimilée légalement à la signature manuscrite.

- Par signature électronique simple, on entend des « données électroniques jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier leur authenticité » (art. 2 let. a SCSE)[48].
- La signature électronique avancée (art. 2 let. b SCSE) doit satisfaire aux exigences d'être liée uniquement au titulaire (identification), de permettre d'identifier le titulaire (authentification), d'être créée par des moyens que le titulaire peut garder sous son contrôle exclusif (sécurité) et

44 Le canton de Zurich (Direction de la Justice et de l'Intérieur) est devenu le premier service d'enregistrement (Registration Authority) à adopter une certification. La plate-forme électronique de passation des marchés publics *simap2* a elle aussi opté pour la signature électronique en vue de permettre la passation de marchés publics en ligne.

45 Message du CF, FF 2001, p. 5429. La communication électronique avec les autorités est déjà une réalité avec l'Administration fédérale des contributions (TVA) ainsi qu'avec l'Institut fédéral de la propriété intellectuelle (dépôts des marques, brevets, etc.).

46 Art. 8 al. 2 Ordonnance FOSC (RS 221.415), qui indique que la certification est fondée sur la SCSE.

47 Ces définitions reprennent la terminologie de la Directive 1999/93/CE du 13 décembre 1999 sur la signature électronique, qui elle-même s'inspire des travaux de la CNUDCI en matière de signature électronique.

48 La plupart des systèmes d'authentification dans le cadre des services bancaires en ligne reposent sur des mots de passe (« one-time passwords »-OTP) ou des jetons à utiliser une seule fois, c'est-à-dire la forme la plus simple de la signature électronique. De nombreuses applications de services bancaires en ligne utilisent ces systèmes aux seules fins d'authentification des utilisateurs.

d'être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable (intégrité).

- Enfin, la **signature électronique** est dite **sûre (ou qualifiée)**, lorsque la signature électronique avancée est fondée sur un **dispositif sécurisé de création et sur un certificat qualifié valable au moment de sa création** (art. 2 let. c SCSE).

c) L'exigence de certificat qualifié

Pour être « qualifié », le certificat permettant de crypter les données doit émaner d'un fournisseur de services de certification lui-même reconnu par un organisme de certification[49]. Pour homologuer la chaîne de certification et de reconnaissance, l'instance suprême suisse est le Service d'accréditation suisse de l'Office fédéral de métrologie. En 2005, lors de l'entrée en vigueur de la loi, aucun fournisseur suisse n'était annoncé et il était nécessaire de passer par des fournisseurs étrangers reconnus en Suisse conformément à l'art. 3 al. 2 SCSE[50]. Dans l'intervalle, deux fournisseurs de services de certifications sont désormais agréés[51-52]. Par contre et à ce jour, seule l'entreprise KPMG est accréditée comme organisme de reconnaissance.

Le certificat numérique ne peut aujourd'hui qu'être délivré à **une personne physique**. Les droits de signature de la personne physique peuvent toutefois être mentionnés dans le certificat (notamment ceux enregistrés auprès du registre du commerce ou résultant d'une représentation par procuration)[53].

Bien que critiquée, cette limitation légale aux personnes physiques trouve sa justification, car, si la loi exige le concours de plusieurs personnes physiques pour engager une personne morale, c'est que chacune d'elles doit confirmer son accord avec le texte qu'elle paraphe. Dans ce cadre, la nécessité d'une signature individuelle et personnelle est dès lors avant tout un garde-fou, notamment lorsqu'un organe doit engager la personne morale qu'il représente. Réunir plusieurs identités physiques (et donc signatures) dans un seul certificat contournerait ces exigences, un seul « signataire électronique » pouvant alors utiliser le certificat pour engager les autres personnes mentionnées dans le certificat, peut-être à leur insu. On relève que des « signatures dématérialisées collectives » existent dans la pratique, mais ne relèvent pas de la signature

49 L'OFCOM a édicté des prescriptions techniques qui précisent les conditions préalables et les exigences essentielles découlant de la loi et de l'ordonnance que doit respecter, afin d'être reconnu, le fournisseur de services de certification qui délivre des certificats électroniques qualifiés ou qui fournit d'autres services en rapport avec les signatures électroniques (RS 943.032.1).

50 Les fournisseurs de services de certification étrangers qui sont reconnus dans un pays dont les exigences de certification correspondent, preuve à l'appui, à celles qui sont appliquées en Suisse sont acceptés (cf. aussi art. 12/2 OelDI). La Confédération a ainsi reconnu les signatures numériques s'appuyant sur un certificat délivré par la société TC TrustCenter AG, accréditée en Allemagne, notamment pour les rapports avec l'Administration fédérale des contributions.

51 Etat au 15 mai 2006.

52 Swisscom solutions (qui vise en priorité les grande entreprises comme les grandes administrations, les banques, assurances, de même que le domaine de la santé) et QuoVadis Limited/QuoVadis Trustlink Schweiz AG (http://www.sas.ch/fr/pki_isms/pki.html). La Poste suisse a déposé une demande de certification qui est en cours d'évaluation auprès de l'organisme de reconnaissance ; elle a en effet annoncé sa volonté de lancer la lettre recommandée électronique dès l'hiver 2006 au plus tôt (http://www.incamail.ch) (cf. infra note 88).

53 Art. 7 al. 2 SCSE et art. 5 al. 2 OSCSE.

électronique qualifiée au sens de la loi et ne sont dès lors pas assimilables à la signature manuscrite[54].

Cette limitation va dès lors poser des problèmes en matière de bail, dès lors que l'une ou l'autre des parties est une personne morale (problématique de la signature collective) ou que le contrat de bail est conclu par une pluralité de bailleurs et/ou de locataires (cf. infra III.2.a).

d) Le régime de responsabilité

Le régime de responsabilité constitue un élément central du système car c'est lui qui pose les bases sur lesquelles se construira la confiance des utilisateurs, ceux-ci devant se fier aux certificats ainsi créés.

1. Des fournisseurs de services de certification et des organismes de reconnaissance

L'art. 16 SCSE règle la responsabilité des fournisseurs de services de certification envers le titulaire de la clé de signature ainsi que vis-à-vis des tiers qui se sont fiés à un certificat qualifié valable. Sans entrer dans trop de détails, la faute du fournisseur et de ses éventuels auxiliaires ne joue aucun rôle (responsabilité causale). La faute concomitante ou propre du titulaire du certificat peut cependant jouer un rôle dans la fixation de l'indemnité (art. 44 CO). On ne peut toutefois réclamer des dommages-intérêts au fournisseur de service pour des faits sur lesquels il n'a aucune influence (rapport de causalité) afin d'éviter de transformer la responsabilité causale en responsabilité pour risque.

L'art. 16 al. 2 SCSE prévoit toutefois un renversement du fardeau de la preuve : il incombe dès lors aux fournisseurs de services de certification d'apporter la preuve qu'ils ont respecté les obligations découlant de la loi et de ses dispositions d'exécution en cas de litige.

Enfin, l'art. 16 al. 3 SCSE interdit aux fournisseurs de services de certification d'exclure leur responsabilité pour leurs certificats qualifiés envers le titulaire de la clé de signature ou à l'égard des tiers. Toute convention ou clause contractuelle contraire (notamment dans des conditions générales) est frappée de nullité (art. 20 al.1 CO)[55].

Le même régime de responsabilité est prévu en cas de défaillance de *l'organisme de reconnaissance* des fournisseurs de services de certification.

2. Des titulaires d'une clé de signature (art. 59a CO nouveau)

Le titulaire d'une clé de signature répond envers les tiers des dommages que ces derniers ont subis parce qu'ils se sont fiés à un certificat qualifié valable délivré par un fournisseur de services

---

54 Notamment dans les contrats de e-banking, où une transaction, pour être exécutée, doit être « validée » par plusieurs signataires devant s'identifier séparément et individuellement sur le site de l'organisme financier.

55 Cette disposition va ainsi plus loin que l'art. 100 al. 2 CO (responsabilité résultant de l'exercice d'une industrie concédée par l'autorité), qui serait à notre sens applicable aux fournisseurs de services de certification (ceux-ci devant être agréés par l'Etat pour délivrer des certificats reconnus par la loi). En application de l'art. 100 al. 2 CO, le juge *pourrait* tenir pour nulle une clause mettant d'emblée à la charge du client, en cas de faute légère du fournisseur de services de certification, le risque de l'exécution en main d'une personne non autorisée à recevoir la prestation (ATF 112 II 450 ss).

de certification reconnu au sens de la SCSE (art. 59a CO). Cette responsabilité relève de la *culpa in contrahendo*[56].

Le titulaire de la clé de signature est libéré de sa responsabilité s'il peut établir de manière crédible qu'il a pris les mesures de sécurité raisonnablement imposées par les circonstances pour éviter une utilisation abusive de la clé de signature. C'est l'art. 11 OSCSE qui définit les mesures de sécurité à prendre au sens de l'art. 59a al. 2[57].

Il y a donc un *renversement du fardeau de la preuve*, justifié par le fait que le tiers qui se fie à un certificat n'a pas la possibilité de contrôler l'usage que le titulaire fait de sa clé de signature. C'est donc ce dernier qui doit convaincre le juge qu'il a conservé sa clé de signature de manière à ce que l'apparence fausse créée vis-à-vis du tiers ne puisse être attribuée à un manquement de sa part, mais à une autre cause[58]. En conséquence, si le titulaire de la clé n'arrive pas à prouver l'absence de tout manquement, il sera tenu pour responsable, même si aucune violation de son devoir de diligence ne sera établie contre lui[59].

La loi n'oblige toutefois pas le tiers à prendre connaissance du certificat ; aucun effet de « publicité positive » n'est attaché au certificat comme avec le Registre du commerce ou le Registre foncier, le principe de la bonne foi (art. 2 al. 1 CC) étant réservé.

Selon le Conseil fédéral, l'art. 59a CO est de droit dispositif[60]; il est probable dès lors que le devoir de diligence du titulaire de la clé sera sans doute aggravé dans les conditions générales contractuelles imposées dans la pratique commerciale.

e) Compatibilité avec le droit européen

La SCSE correspond aux exigences du droit européen, dont elle reprend certaines définitions. La loi fédérale va même plus loin puisqu'elle ne met aucune restriction à la conclusion d'un contrat sous forme électronique[61].

Pour faciliter l'utilisation et la reconnaissance juridique internationales des signatures électroniques, le Conseil fédéral peut conclure des conventions internationales portant notamment

---

56 Message du CF, FF 2001, p. 5451.

57 Le titulaire d'un certificat qualifié ne doit confier le dispositif de création de signature à personne. Dans la mesure de ce qui peut être exigé, il doit garder ce dispositif en sa possession ou le mettre en lieu sûr. En cas de perte ou de vol du dispositif de création de signature, le titulaire d'un certificat qualifié doit demander l'annulation de ce dernier dans les meilleurs délais. Il en va de même pour le titulaire qui sait ou qui a des raisons de croire qu'un tiers a pu avoir accès à la clé de signature. Les données d'activation du dispositif de création de signature (données d'activation) ne doivent pas se référer à des données personnelles du titulaire d'un certificat qualifié. Les transcriptions des données d'activation doivent être conservées en lieu sûr et séparément du dispositif de création de signature. Le titulaire d'un certificat qualifié doit modifier les données d'activation lorsqu'il sait ou qu'il a des raisons de croire qu'un tiers en a eu connaissance. S'il ne peut pas lui-même modifier les données d'activation, il doit demander l'annulation du certificat dans les meilleurs délais. (Art. 11 OSCSE, RS 943.032).

58 Message du CF, FF 2001, p. 5451.

59 Langer, Verträge mit Privatkunden im Internet, p. 239-240.

60 Message du CF, FF 2001, p. 5451.

61 L'art. 9 Directive 2000/31/CE du 8 juin 2000 (Directive sur le commerce électronique) stipule que l'interdiction de discriminer le commerce électronique ne s'applique pas, entre autres, aux contrats qui créent ou transfèrent des droits sur des biens immobiliers, *à l'exception des droits de location (*en d'autres termes, les Etats membres ne peuvent édicter de dispositions légales restreignant la conclusion des contrats de bail immobilier) ; MCF FF 2001, p. 5430 et 5456.

sur la reconnaissance des signatures électroniques et des certificats, ainsi que sur la reconnaissance des fournisseurs et l'accréditation des organismes de reconnaissance (art. 19 LSCE).

5. Assimilation de la signature électronique qualifiée à la signature manuscrite

Seule la signature électronique *avancée qualifiée* est assimilée à la signature manuscrite (art. 14 al. 2 bis CO), c'est-à-dire la signature électronique fondée sur un dispositif sécurisé de création de signature et sur un certificat qualifié valable au moment de sa création (art. 2 let. c SCSE).

Les nouvelles dispositions légales assimilent totalement la signature électronique qualifiée à la signature manuscrite, sans prévoir d'exceptions.

La signature électronique qualifiée ne remplace que la signature manuscrite exigée dans la forme écrite liée au support papier (forme écrite simple). En conséquence, la forme authentique n'est pas touchée (art. 55 Tit. fin. CC), contrairement à d'autres pays comme la France, où les notaires sont habilités à passer des actes authentiques électroniques depuis le 1er février 2006[62]. La signature électronique qualifiée ne peut également se substituer à des indications écrites à la main (par exemple l'art. 493 al. 2 CO, indication manuscrite du montant de la garantie lors d'un cautionnement par une personne physique qui ne dépasse pas 2000 francs) ou à un document écrit de la main de son auteur (p. ex. l'art. 505 CC concernant le testament olographe).

En contrepartie de cet élargissement[63], le Conseil fédéral entendait intégrer la protection légitime de la partie faible au contrat, garantie par la forme écrite traditionnelle, dans une loi fédérale sur le commerce électronique, dont il avait mis l'avant-projet en consultation en même temps que celui sur la loi fédérale sur la signature électronique[64]. Cet avant-projet prévoyait, entre autres, un droit de révocation pour les contrats conclus à distance et améliorait la position du consommateur qui achetait des biens de consommation[65].

---

62 Les actes authentiques électroniques dressés par les officiers publics sont signés au moyen d'une signature électronique sécurisée mais certains actes conservent les vestiges de « l'acte papier » puisque « pour leur signature, les parties et les témoins doivent utiliser un procédé permettant l'apposition sur l'acte notarié, visible à l'écran, de l'image de leur signature manuscrite ». Pour tenir compte d'un environnement où support papier et support électronique coexisteront, les textes prévoient la possibilité de numériser des documents papier pour les annexer à des actes ou d'adjoindre à un acte des documents d'origine électronique (tels que des actes établis par d'autres officiers publics, des photos, vidéos ou enregistrements numériques). Des copies authentiques ou expéditions des actes peuvent être établies sur support papier ou sur support électronique, quel que soit le support initial de l'acte. Un huissier peut également re-matérialiser l'acte authentique sur support électronique aux fins de signification ou d'exécution (Sabine Lipovetsky, Les actes authentiques se dématérialisent enfin, Journal du net, 20/09/05 ; Forum des droits sur l'Internet, Actes authentiques électroniques : les notaires et les huissiers entrent pleinement dans le numérique, 23/08/2005).

63 La protection de la partie faible a été vivement discutée lors de l'adoption de la SCSE au Parlement et une motion voulait restreindre l'utilisation de la signature électronique en matière de contrats de travail, de bail ou dans le cadre du droit de la consommation ou du leasing (BOCE 2003, p. 851) (http://www.parlament.ch/ab/frameset/d/s/4620/89212/d_s_4620_89212_89213.htm).

64 Révision partielle du droit des obligations et de la loi fédérale contre la concurrence déloyale, FF 2001, p. 5431.

65 Jaccard, Le législateur suisse à l'épreuve d'Internet : aperçu de l'avant-projet de loi fédérale sur le commerce électronique, in : SJ 2003 II 209 ss.

Contre toute attente, le Conseil fédéral a abandonné le 9 novembre 2005 le projet de loi fédérale sur le commerce électronique, considérant qu'une extension de la protection des consommateurs n'était finalement pas nécessaire[66].

6. Problématique de la preuve numérique et de sa conservation

a) Principe

La conclusion d'actes juridiques par la voie électronique fait inévitablement naître chez le praticien la question de la preuve en cas de litige ultérieur. La dématérialisation de la transaction entraîne en effet un sentiment d'insécurité chez les parties.

Dans le système de la libre appréciation des preuves qui prévaut dans l'ordre juridique suisse, tous les moyens de preuve, même les indices, sont susceptibles d'emporter la conviction du juge car ce dernier décide selon son intime conviction si un fait est établi ou non[67]. Lorsque le droit fédéral ne prévoit pas de forme particulière pour un engagement juridique, le droit cantonal de procédure ne peut faire dépendre d'une forme particulière la preuve de cet engagement (art. 10 CC)[68]. Le juge apprécie donc souverainement la valeur des éléments de preuve régulièrement produits au cours du procès[69]. En conséquence, *aucune preuve ne peut être refusée au seul motif qu'elle résulte d'un enregistrement électronique ou qu'elle est présentée sous forme informatique*[70].

Certes, la force probante d'un document signé est importante et pèse de manière significative lors de l'appréciation des preuves par le juge. Avec l'assimilation de la signature électronique qualifiée à la signature manuscrite, les documents signés électroniquement conformément aux exigences légales auront désormais autant de force probante que les documents en la forme écrite simple.

L'avant-projet de loi fédérale de procédure civile fédérale mentionne explicitement que les données électroniques ont la même valeur que les titres ordinaires, afin de lever certaines ambiguïtés rencontrées dans les droits de procédure cantonaux actuels[71].

Les signatures électroniques qui ne sont pas qualifiées (au sens de la SCSE) ne sont pas pour autant dépourvues de toute force probante[72]. La force probante des courriers électroniques non munis d'une signature électronique dépendra des contestations qui pourront être soulevées,

---

66 http://www.ofj.admin.ch/bj/fr/home/themen/wirtschaft/gesetzgebung/abgeschlossene_projekte/konsumentenschutz.html

67 ATF 115 IV 267 = JT 1991 IV 145 cons. 1.

68 Langer, Verträge mit Privatkunden im Internet, Zurich 2003, p. 235.

69 Walder-Richli, Zivilprozessrecht, Zurich 1996, p. 343 n° 132, Hohl, Procédure, p. 213 n° 1107 ss.

70 Rapport explicatif de l'avant-projet du Conseil fédéral sur la LF sur la signature électronique, janvier 2001, p. 7 ; Rihm, E-Mail als Beweismittel im Zivilgerichtsverfahren, RSJ 96 (2000), p. 499; Bühler, op. cit., p. 76.

71 Cf. notes 19 et 20 ; Fanger, Digitale Dokumente als Beweis im Zivilprozess, Bâle 2005, p .122 ss; Langer, Verträge mit Privatkunden im Internet, Zurich 2003, p. 232.

72 Il existe différentes classes de certificats émis par les autorités de certification, en fonction du service associé et des assurances offertes (les certificats de classe 3 offrent le plus de garantie, sur l'identité du possesseur de la clé privée, parce que l'enregistrement nécessite une présence physique).

notamment quant à leur émission, réception, intégrité et imputabilité à l'auteur du message[73]. En cas de contestation, celui qui entendra se prévaloir de sa signature devra apporter la preuve de sa fiabilité, ce qui pourrait déboucher sur une procédure coûteuse.

b) Production de la preuve numérique en justice

Les parties, outre le dépôt de l'information numérique et de son support, y ajouteront par principe une version imprimée de la preuve numérique, dans la mesure où il s'agit d'informations destinées à être lues (et non être entendues ou vues)[74].

En effet, les tribunaux peuvent exiger la production des supports électroniques sous forme écrite (« de manière à être lisibles sans l'aide d'instruments ») ou que soient mis à leur disposition les moyens nécessaires pour les rendre lisibles en audience[75], en vertu du principe d'immédiateté. Avec la généralisation de l'informatique, y compris dans les greffes des tribunaux, ces derniers possèdent désormais les moyens de procéder à l'exécution de la preuve numérique pour prendre connaissance de son contenu[76]. Certains codes prévoient déjà que le juge ordonne les mesures appropriées pour la reproduction s'agissant d'un film ou d'un autre moyen de reproduction sonore ou visuel[77].

D'autre part, tant le tribunal que l'adverse partie peuvent exiger la preuve de l'origine et de l'authentification du document électronique, qui se fera nécessairement par le dépôt des données numériques liées indissociablement à leur support, puisque seul ce dépôt constitue la preuve originale.

On relève au passage que la récente réforme de l'organisation judiciaire fédérale permettra aux mandataires de communiquer avec les instances judicaires par la voie électronique dès le 1er janvier 2007, et à ces instances de notifier leurs décisions également par la voie électronique[78].

---

73 Une comparaison peut être faite avec la télécopie, dont l'usage est courant, alors qu'elle ne constitue pas un écrit original signé. En pratique, les contestations tendent à porter davantage sur le contenu de l'accord et ses conditions d'exécution que sur l'existence même de la transaction conclue par télécopie, dont le principe général n'est généralement pas remis en cause. Il semble en aller de même avec le courriel.

74 Selon entretien de l'auteur avec un juge du Tribunal de district à Neuchâtel (9 septembre 2005), il est désormais fréquent que des courriels soient déposés en procédure uniquement sous leur version imprimée et à ce jour, aucune contestation relative à leur authenticité n'a été soulevée. Sans doute là également, les litiges portent plus sur le contenu du courriel que de sa forme.

75 Rihm, E-Mail als Beweismittel im Zivilgerichtsverfahren, RSJ 96 (2000), p. 497-504, p. 499.

76 La standardisation des formats de fichiers rend la lecture de ceux-ci indépendante du système de lecture. Cela permet ainsi une harmonisation des échanges d'informations électroniques (et donc aussi une meilleure sécurité des échanges).

77 Art. 176/3 CPCVd.

78 Projet JusLink (http://www.juslink.ch/doc/Art_JusLink_fr.pdf): Dès le 1er janvier 2007, le Tribunal fédéral, le Tribunal pénal fédéral et le Tribunal administratif fédéral autoriseront l'envoi de mémoire sous une forme électronique et notifieront leurs jugements également sous une forme électronique à tous ceux qui auront donné leur accord à cette manière de faire. Les modules peuvent être utilisés et seront utilisés par d'autres entités administratives à l'échelon fédéral, cantonal et communal pour permettre des transactions électroniques en matière de poursuites, de demandes d'autorisations, d'impôts, de requêtes concernant des registres.

c) Fragilité et volatilité du support

Loin de son objectif initial de réduction des volumes et d'organisation de l'archivage papier, *l'archivage électronique* est devenu le corollaire indispensable de la dématérialisation du droit, pour ce qui concerne notamment le droit de la preuve et le droit des contrats[79]. En effet, peu importe la validité de l'acte initial, si aucune preuve fiable ne peut être apportée ultérieurement. Il est donc nécessaire de conserver, avec le support de stockage, son format physique d'organisation des données[80].

La particularité de l'information numérique, à savoir de ne pas avoir de caractéristique physique utilisable pour l'identifier, rend sensible l'argument consistant à remettre en cause la preuve sous prétexte qu'elle aurait été altérée. Les preuves doivent être protégées contre les risques de dégradation, de contamination ou d'altération, afin de sauvegarder ses caractéristiques premières et ainsi garantir leur intégrité et leur authenticité. La conservation des preuves numériques passe par trois processus essentiels : la qualité de la collecte, la limitation de leur dégradation naturelle et la préservation de toute contamination[81].

La durée de vie des applications logicielles et des plates-formes techniques est parfois beaucoup plus courte que celle du support lui-même. Les supports, quant à eux, connaissent une évolution parallèle. Le signal y est enregistré de façon de plus en plus dense et le support est de plus en plus fragile. La qualité des supports amovibles (par ex. DVD, CD, disquettes) s'est largement dégradée au fil du temps et il n'est pas rare qu'un CD-R ou DVD-R soit illisible après une année. La lecture nécessite un intermédiaire technique. Cette intermédiation est un nouveau point de vulnérabilité pour la conservation, car, à côté du support, il faudrait pouvoir conserver le support de lecture[82].

Afin d'éviter de se retrouver avec des supports illisibles par les machines actuelles, la technique de la migration des données offre une solution au problème soulevé ci-dessus[83]. Ce point est très important dans l'optique de procédures judiciaires qui peuvent durer des mois, voire des années. De nombreuses directives existent en relation avec l'archivage électronique, afin de conserver en particulier la preuve de l'intégrité des données[84].

---

79 Gasser/Häusermann/Müller, E-mail im Wechselspiel von Informationstechnologie und Recht, in: www.swisslex.ch , 19 mai 2006.

80 Blandine Poidevin, L'archivage électronique, http://www.jurisexpert.net, 5 mai 2006.

81 Lathoud, La gestion formelle de la trace informatique : un moyen de renforcer la politique de sécurité d'un système d'information, Thèse, Lausanne 2002, p. 136.

82 Rodes/Piejut/Plas, La mémoire de la société de l'information, Unesco, 2003, p. 47-49 (http://unesdoc. unesco.org/images/0013/001355/135529f.pdf).

83 « Cette technique consiste à recopier des données numériques d'un support devenu obsolète sur un support récent, de manière à faire persister les données électroniques et cela, au fur et à mesure de l'évolution des techniques. Cette migration peut s'établir également au niveau du format de fichier ou du système d'exploitation. Une telle solution est évidemment très coûteuse, étant donné le coût du nouveau support et le temps de recopie non négligeable », Lieutenant/Marin, Archivage et Horodatage de documents électroniques, Centre de Recherches Informatique et Droit, p. 8 (http://www.droit.fundp.ac.be/e-justice/documents/archivage-horodatage.pdf).

84 Lathoud, La gestion formelle de la trace informatique : un moyen de renforcer la politique de sécurité d'un système d'information, Thèse, Lausanne 2002, p. 138. L'Administration fédérale des contributions émet les recommandations suivantes afin d'assurer la pérennité des données électroniques, dont on pourrait largement s'inspirer dans le cadre de

Avec le développement des réseaux informatiques, la menace provenant de l'extérieur du système sur lequel l'information numérique est stockée ne doit pas non plus être minimisée et les mesures de sécurité qui s'imposent doivent être prises en conséquence (antivirus, *firewalls*, redondance des sauvegardes, mesures d'authentification pour accéder aux données, etc.). Dans l'idéal, les données devraient être conservées sur des supports séparés et indépendants. Les menaces physiques, qui planent également au-dessus des preuves classiques, doivent également être prises en compte (incendie, dégâts d'eau, destruction involontaire, malveillance, etc.)[85].

d) Une solution ? La lettre recommandée électronique avec accusé de réception (« cachet postal électronique »)

Malgré l'utilisation de la signature électronique, rien ne garantit que le message soit bien *parvenu* à son destinataire et la question de la preuve demeure récurrente. Certes, l'expéditeur peut toujours activer la fonction « accusé de réception » (voire même une fonction « confirmation de lecture ») lorsqu'il envoie le message signé via son serveur de mail ; toutefois, à réception, le destinataire peut librement refuser de délivrer une telle confirmation.

Pour répondre à cette demande, des systèmes de « cachet postal électronique » sont proposés par des entreprises privées[86], voire désormais les postes nationales[87-88]. La Poste suisse envisage de lancer son système « Incamail », actuellement en phase test, durant l'hiver 2006[89].

La structure mise en place, qui repose aussi sur une PKI, présente les mêmes caractéristiques que le trafic postal réel :

- l'expéditeur du message électronique s'identifie auprès du prestataire de services (auprès duquel il est enregistré et dispose d'un certificat qualifié) ;
- le message est rédigé (soit sur un serveur web du prestataire ou via un serveur mail classique de messagerie électronique) et chiffré (enveloppe numérique);

---

la preuve (Commentaire de l'Ord. du DFF concernant les données et les informations transmises par voie électronique (Oeldi) du 30 janvier 2002, p. 9 ; http://www.estv.admin.ch/data/mwst/f/egv/pdf/commentaire.pdf):

- Sauvegarder périodiquement les données sur un nouveau support ;
- Convertir ou transférer périodiquement les données, c'est-à-dire les convertir dans un autre format ;
- Conserver les anciens systèmes nécessaires à la lecture des données en les réinstallant sur des nouveaux systèmes de gestion des données (émulation) ;
- Enregistrer les données sous un format basé sur un standard reconnu d'une manière générale et dont les spécifications sont accessibles à tous, par ex. le format XML (*Extensible Markup Language*).

85 Ghernaouti, Sécurité Internet, Stratégies et technologies, Paris, 2000, p. 53ss.

86 Montero, Du recommandé traditionnel au recommandé électronique : vers une sécurité et une force probantes renforcées, in : *Le commerce électronique : de la théorie à la pratique*, Bruxelles, 2003, p. 69-99 publié sur http://www.droit-technologie.org/2_1.asp?dossier_id=102 conseille de demeurer prudent avec les fournisseurs privés, certains services étant nettement sujets à critique).

87 Les systèmes proposés par Les Postes française et belge ne sont qu'à moitié dématérialisés : le fichier transmis est imprimé par La Poste puis distribué sous forme de courrier traditionnel par le facteur (pour le fonctionnement : http://www.laposte.fr/LRE/index.html et http://www.mycertipost.be/fr/Recommande.html).

88 Le coût de l'utilisation du système dépendra du coût d'acquisition d'un certificat numérique, puis du coût de l'utilisation par envoi ; le système combiné français débute à 4.97 € pour une lettre d'une page. En Belgique, il se monte au minimum à 9,84 € TTC.

89 http://www.incamail.ch

- le message transite par le prestataire, qui envoie à l'expéditeur un « récépissé » prouvant l'envoi, l'identité de l'expéditeur, l'adresse du destinataire, ainsi que la date et l'heure de l'envoi (horodatage) ; cela équivaut à « la preuve de l'envoi » ;
- le destinataire peut accéder au message en passant par une étape d'identification préalable ;
- lorsque le destinataire télécharge le message, un accusé de réception est envoyé par le prestataire aux deux parties, prouvant la date et l'heure à laquelle le destinataire a pris connaissance du message électronique (« preuve de la réception »).

La preuve de dépôt électronique[90] permet d'attester de l'envoi d'une lettre recommandée électronique, ainsi que de son contenu, grâce à la signature numérique et la fonction de hachage. A cet égard, le recommandé électronique apporte une fonction supplémentaire appréciable par rapport au recommandé traditionnel.

La Poste suisse envisage de proposer les deux produits : la lettre recommandée électronique avec accusé de réception, ainsi que la lettre électronique simple avec « preuve de remise »[91].

III. Conséquences de l'introduction de la signature électronique en droit du bail

1. La conclusion du contrat de bail

a) Mécanisme de conclusion

Comme le contrat de bail est valablement conclu sans qu'il soit nécessaire de respecter une forme spéciale, les contrats conclus par voie électronique doivent être par conséquent, d'un point de vue formel, considérés comme valables dès lors que les parties ont manifesté leur volonté conformément à l'art. 1 al. 1 CO[92], soit par l'échange de manifestations de volonté réciproques et concordantes, portant sur le contenu essentiel du contrat (outre les parties, l'objet du bail et la rémunération)[93].

S'agissant de l'échange des consentements et conformément à la doctrine dominante[94], une annonce pour un bien à louer sur un site Internet n'est qu'une *invitation à formuler une offre* au

---

90 Les informations contenues dans la preuve électronique de dépôt sont :
- Les coordonnées de l'expéditeur et du destinataire indiquées par l'expéditeur au moment de son envoi.
- Les caractéristiques de la lettre recommandée : nom, taille et empreinte du fichier d'édition.
- La date et l'heure de dépôt au sein du cachet électronique.
- Les informations techniques identifiant le prestataire et son service.

91 Les prix provisoires annoncés seront de CHF 2.50 pour la lettre recommandée électronique (jusqu'à 1 méga) et de CHF 0.50 pour la lettre électronique avec preuve de remise (jusqu'à 250ko, puis CHF 0.70 jusqu'à 1 méga, puis CHF 0.40 par méga supplémentaire).

92 Cherpillod Giacobino, Internet dans la conclusion du contrat et les solutions de paiement, in : SJ 2003 II, p. 393-434, p. 406.

93 Tercier, les contrats spéciaux, Zurich 2003, 3e éd., p. 264 n° 1806.

94 Jaccard, La formation des contrats sur Internet et la vente aux enchères en ligne, in : Quelques facettes du droit de l'Internet, volume 1, Neuchâtel 2001, p. 56 ; Briner, Verträge und Haftung im Internetrecht, Zurich 2002, p. 38, qui compare le site à un « catalogue » ; Favre-Bulle, Le Contrat électronique, in : Le contrat dans tous ses états, Berne 2004, p. 186 et réf. de la note 44.

sens de l'art. 7 al. 2 CO[95]. Un des critères tient notamment au fait qu'en cas de solution contraire, le bailleur perdrait tout contrôle sur l'attribution du bien et n'aurait pas l'occasion, entre autres, de vérifier préalablement la solvabilité du locataire. En revanche, si le bailleur adresse un courrier électronique à un locataire potentiel contenant tous les éléments objectivement et subjectivement essentiels, il s'agit bien d'une offre.

L'offre et l'acceptation sont des déclarations de volonté soumises à réception. En tant que telles, elles doivent être considérées comme reçues dès qu'elles entrent dans la sphère juridique de leur destinataire[96]. Lorsqu'elles sont envoyées par l'intermédiaire d'Internet, elles doivent donc être considérées comme telles dès que leur destinataire peut avoir accès à elles, c'est-à-dire dès qu'elles sont entrées dans le système désigné par le destinataire, même si celui-ci est géré par un tiers[97].

En principe, le destinataire d'une offre faite par le biais d'Internet (échange de courriers électroniques, appui d'une touche du clavier ou clic de souris) ne peut réagir directement à l'offre. Celle-ci doit donc être considérée comme faite entre absents[98]. En vertu de l'art. 5 al. 1 CO, l'offre doit être acceptée dans un délai raisonnable ; compte tenu de la vitesse des communications sur Internet, ce délai est relativement court[99]. En revanche, si les parties sont « en direct » (*chat,* forum, téléphonie IP par exemple), l'offre est considérée comme faite entre présents, indépendamment du décalage temporel ou de l'absence de rencontre physique et l'acceptation doit

---

95 Cf. par exemple les restrictions posées par le portail www.homegate.ch (http://www.homegate.ch/homegate/disclaimer?articleId=UE-legal-discl&level1=default&level2=default&level3=default): « Pas d'offre » : Les informations publiées dans homegate.ch ne justifient ni une demande d'offre, ni une offre ou une recommandation pour la location, […]. Toutes les données ont lieu sans garantie (*sic*).

96 Bohnet, Les termes et délais en droit du bail à loyer, 13e Séminaire sur le droit du bail, Neuchâtel 2004, p. 4 s.

97 Cherpillod Giacobino, Internet dans la conclusion du contrat et les solutions de paiement, SJ 2003 II, p. 393-434, p. 409 ; Jaccard, La formation des contrats sur Internet et la vente aux enchères en ligne, in : Quelques facettes du droit de l'Internet, volume 1, Neuchâtel 2001, p. 61 ; Probst, Le droit du bail et Internet, in : 11e Séminaire sur le droit du bail, Neuchâtel 2000, p. 13 et note 52 ; selon Briner (Verträge und Haftung im Internetrecht, Zurich 2002, p. 39) à mesure que le destinataire a désigné une adresse électronique, on peut attendre de lui qu'il relève régulièrement sa boîte aux lettres électronique, tout comme il est censé le faire avec son courrier postal traditionnel.

Selon l'art. 15 de la Loi-type de la CNUDCI sur le commerce électronique, Guide, New-York, 1999, p. 56 ss (http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf), l'expédition intervient lorsque le message de données entre dans un système d'information ne dépendant pas de l'expéditeur tandis que le moment de la réception est défini lorsque le message entre dans le système d'information désigné par le destinataire ; si le message est envoyé à un autre système d'information que celui désigné, c'est le moment où il est relevé qui est déterminant . Par l'expression "système d'information désigné", la Loi type vise un système qui a été expressément désigné par une partie, par exemple lorsqu'une offre indique expressément l'adresse à laquelle l'acceptation devrait être envoyée. La simple mention de l'adresse du courrier électronique ou de la télécopie sur un en-tête ou autre document ne devrait pas être considérée comme désignant expressément un ou plusieurs systèmes d'information. En particulier, lorsque le système d'information du destinataire ne fonctionne pas ou fonctionne mal, ou, bien que fonctionnant convenablement, n'est pas en mesure de recevoir le message de données (par exemple dans le cas d'un télécopieur constamment occupé), l'expédition ne se produit pas.

98 Jaccard, La formation des contrats sur Internet et la vente aux enchères en ligne, in : Quelques facettes du droit de l'Internet, volume 1, Neuchâtel 2001, p. 61 ; Favre-Bulle, Le Contrat électronique, in : Le contrat dans tous ses états, Berne 2004, p. 187.

99 Le lendemain ou le surlendemain : Probst, Le droit du bail et Internet, in : 11e Séminaire sur le droit du bail, Neuchâtel 2000, p. 12 et note 48 ; Briner, Verträge und Haftung im Internetrecht, Zurich 2002, p. 39.

avoir lieu immédiatement[100]. Le contrat est dès lors conclu par Internet dès que le destinataire de l'offre envoie son acceptation (art. 10 al. 1 CO)[101].

En conséquence, et comme l'avait déjà mentionné en 2000 dans ce séminaire Probst[102], un contrat de bail peut ainsi se conclure de manière totalement dématérialisée, notamment par un échange de courriers électroniques ou par un échange informatisé via un formulaire électronique à remplir en ligne, à mesure que ceux-ci contiennent les éléments essentiels du contrat.

Il n'est donc pas nécessaire de recourir à la signature électronique. En revanche, la signature électronique amène une sécurité supplémentaire, en particulier en matière de preuve (supra, II.6). On notera également qu'un document signé électroniquement vaut reconnaissance de dette au sens de l'art. 82 LP[103].

En pratique, la majorité des baux respecte aujourd'hui la forme écrite, non seulement à des fins de preuve, mais également pour régler et aménager de manière détaillée les relations contractuelles entre les parties. Cette réserve de la forme écrite (art. 16 CO) peut être expresse ou résulter d'actes concluants, notamment lorsque une partie remet à l'autre deux exemplaires de contrat à signer. Dans ce cas, le contrat ne sera conclu que lorsque les règles de la forme écrite auront été respectées[104].

En matière de signature électronique, l'envoi par le bailleur d'un contrat signé électroniquement à la boîte électronique du locataire indiquerait sa volonté de n'être lié que par la forme écrite. Le locataire pourrait toutefois notifier son acceptation au bailleur soit en renvoyant lui-même le contrat sous format électronique en le verrouillant avec sa propre signature électronique, soit en l'imprimant et en renvoyant le texte signé de sa main par courrier postal traditionnel.

---

100 Alors que Jaccard (Le législateur suisse à l'épreuve d'Internet : aperçu de l'avant-projet de loi fédérale sur le commerce électronique, in : SJ 2003 II 214) réservait encore prudemment des hypothèses particulières tels forums de discussion en temps réel ou de retransmission audiovisuelle (instant messaging, webcam, chat), on doit aujourd'hui admettre par exemple sans aucune hésitation que la VoIP permet la conclusion de contrat entre présents (d'accord sur ce dernier point : Favre-Bulle, Le Contrat électronique, in : Le contrat dans tous ses états, Berne 2004, p. 187).

101 Contrairement au droit européen (Directive 1997/7/CE du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance), le droit suisse ne prévoit de lege lata ni possibilité de révoquer un contrat conclu par voie électronique, ni aucun mécanisme particulier relatif à la passation de commande, malgré la (trop grande) facilité avec laquelle il peut parfois être conclu. L'art. 11 de la Directive 2000/31/CE sur le commerce électronique assigne un rôle particulier à l'accusé de réception et exige un mécanisme de correction des erreurs de saisie et ce, avant la passation de la commande. Cette disposition ne s'applique toutefois pas aux contrats exclusivement passés au moyen d'un échange de courriers électroniques ou au moyen de communications individuelles équivalentes. L'art. 10 impose également un devoir d'information précontractuel au prestataire.

102 Probst, Le droit du bail et Internet, in : 11e Séminaire sur le droit du bail, Neuchâtel 2000, p. 9.

103 Guggenheim, Commentaire Romand, n° 6 ad art. 15 CO; Cerruti, La protection de la partie faible et la loi sur la signature électronique, Bulletin Cedidac n° 40, Novembre 2004, Lausanne, p. 2; Message du CF, FF 2001, p. 5432.

104 Lachat, Le bail à loyer, Lausanne 1997, p. 115 n° 4.1.3.

b) Inclusion de conditions générales

Les conditions générales jouent un rôle important en matière de baux immobiliers; la plupart des contrats écrits y faisant référence. Il s'agit dès lors de déterminer comment celles-ci peuvent être intégrées dans un échange de consentements dématérialisés.

Si le contrat est conclu via un site web, le texte effectif des conditions générales doit être publié et facilement consultable avant la conclusion du contrat[105]. Un lien hypertexte peut être admissible si le renvoi est suffisamment clair. Les conditions générales doivent pouvoir être téléchargées ou à tout le moins imprimées, de façon à permettre au consommateur de matérialiser ces clauses sur un support durable[106]. Il est recommandé d'insérer une étape dans la conclusion du contrat dématérialisé, en obligeant l'internaute à cocher une case indiquant qu'il a pris connaissance des conditions générales, voire à l'obliger également à dérouler le texte des conditions générales avant de passer à l'étape suivante en vue de la finalisation du contrat.

Si le contrat est conclu par l'échange de consentements via des courriers électroniques signés, le fichier contenant les conditions générales devrait être intégré au message contenant les éléments de l'offre, de manière à ce que le locataire puisse en prendre connaissance avant de donner son consentement. On peut s'interroger si l'intégration des conditions générales serait considérée comme suffisante si le contrat électronique ne contient qu'un hyperlien renvoyant au site web du bailleur, sur lequel les conditions générales pourraient être consultées et enregistrées[107].

2. Déclarations de volonté et exercice de droits formateurs

Une fois le contrat de bail conclu, celui-ci va prendre vie et évoluer, à mesure qu'il est par définition un contrat de durée. Certaines manifestations de volonté des parties, en particulier l'exercice de droits formateurs, doivent parfois respecter des formes particulières[108].

a) Titularité et exercice

Si les parties au contrat de bail sont individuelles, l'exercice de droits formateurs liés au rapport d'obligation, à l'instar de la résiliation du bail, ne pose pas de problème particulier, y compris par le biais de la signature électronique.

En revanche, en cas de bail commun, ces droits doivent être exercés en commun par toutes les personnes physiques ou morales qui constituent une seule et même partie ou contre elles

105 Le droit suisse n'exige pas une prise de connaissance effective des conditions générales, ni le respect d'une forme particulière, à quelques exceptions près qui ne concernent pas le droit du bail: Langer, Verträge mit Privatkunden im Internet, Zurich 2003, p. 354-355.

106 Favre-Bulle, Le Contrat électronique, in : Le contrat dans tous ses états, Berne 2004, p. 189.

107 Le bailleur devrait en outre avoir expressément avoir attiré l'attention du locataire sur l'existence des conditions générales: Langer, Verträge mit Privatkunden im Internet, Zurich 2003, p. 355 et réf. citées à la note 28.

108 Probst, Le droit du bail et Internet, in : 11e Séminaire sur le droit du bail, Neuchâtel 2000, p. 17.

toutes[109]. Un contrat de bail commun est un rapport juridique uniforme qui n'existe que comme un tout et pour tous les participants.

Les cobailleurs peuvent confier à un représentant autorisé le soin d'exercer un droit formateur[110]. La jurisprudence s'est surtout penchée sur la problématique de la résiliation du bail en cas de communauté de bailleurs[111]. Naturellement, des colocataires peuvent également exercer un droit formateur par le biais d'un représentant autorisé.

En matière de signature électronique, la problématique de la signature collective a été abordée plus haut (supra cf. II.4.c). Un représentant dûment autorisé pourrait ainsi valablement exercer un droit formateur par la voie électronique pour le compte de la communauté de bailleurs ou de locataires. A notre sens, dans la mesure où il ne s'agit pas d'un droit de signature issu d'une personne morale, le pouvoir de représentation n'a pas besoin de ressortir du certificat qualifié.

A l'inverse, si une partie doit exercer un acte formateur par la voie électronique à l'encontre d'une communauté de co-contractants, elle devra préalablement obtenir que soit désigné un représentant commun pour lui adresser son courrier électronique signé (ce qui dans la pratique est généralement le cas)[112]. Toutefois, ce courrier devra être clairement libellé à l'égard de l'ensemble des cocontractants, par le biais du représentant. La problématique de la protection du logement de la famille est toutefois réservée, certains avis devant être notifiés séparément au conjoint par le bailleur[113].

b) Absence de forme particulière requise

Si aucune forme particulière n'est requise, on en déduit a fortiori que le recours à la signature électronique ne pose aucun problème particulier. On peut citer par exemple le locataire qui doit signaler à son bailleur l'existence de défauts (art. 257g CO), le consentement du bailleur à la sous-location (art. 262 CO), etc. Le recours à la signature électronique permettra d'élever la force probante de la déclaration ainsi faite, au contraire d'une déclaration orale ou par actes concluants, par exemple.

---

109 4C.17/2004 Arrêt du 2 juin 2004 ; ATF 4C.331/1993 du 20 juin 1994, consid. 2b, publié in SJ 1995, p. 53 ss cons. 5b et réf. citées ; Jacquemoud Rossari, Jouissance et titularité du bail ou quelques questions choisies en rapport avec le bail commun, in CdB 1999, p. 97 ss, 100 ; RJN 1995, p. 53-54. Par exemple, le congé qui n'émane pas de la totalité ou de la majorité requise des cobailleurs ou qui émane d'un représentant non autorités est nul (Lachat, Le bail à loyer, p. 412 n. 6.2).

110 Lorsque ce représentant est un des membres de la communauté, il doit être autorisé, c'est-à-dire avoir reçu le pouvoir de résilier le bail selon les règles régissant les rapports au sein de cette communauté. Il n'est pas nécessaire que le rapport de représentation ressorte de l'avis même de résiliation; conformément à l'art. 32 al. 2 CO, il suffit que le locataire ait dû inférer des circonstances qu'il existait un rapport de représentation ; Higi, Commentaire zurichois, n. 71 ad Remarques préalables aux art. 266-266o CO.

111 Jacquemoud Rossari, Jouissance et titularité du bail ou quelques questions choisies en rapport avec le bail commun, in : CdB 4/99, p. 103-104.

112 Une telle pratique est ainsi admise pour la notification d'une hausse de loyer à des colocataires. S'agissant de la notification du congé, celui-ci peut être adressé à un représentant commun, pour autant que le contrat prévoit la désignation d'un représentant commun (Jacquemoud Rossari, Jouissance et titularité du bail ou quelques questions choisies en rapport avec le bail commun, in : CdB 4/99, p. 104).

113 Notamment la résiliation du bail par le bailleur (art. 266n CO) ou l'avis comminatoire de l'art. 257d CO.

c) Forme écrite requise

Lorsque le droit du bail exige la forme écrite pour une déclaration ou un acte formateur[114], ceux-ci peuvent être effectués de manière dématérialisée en recourant à la signature électronique reposant sur un certificat qualifié, afin de respecter les exigences de la forme écrite.

d) Le cas particulier de la formule officielle

La loi impose le recours à une formule officielle dans plusieurs cas : congé donné par le bailleur (art. 266l al. 2 CO), notification de hausse de loyer ou de nouvelles prétentions (art. 269d al.1 et 3 CO), notification du loyer initial lors de la conclusion du bail dans les cantons où celle-ci a été rendue obligatoire en raison de la pénurie de logements (art. 270 al. 2 CO). Le bailleur peut-il dès lors notifier cette formule par voie électronique ?

Dans son message sur la future SCSE, le Conseil fédéral estimait qu'il appartiendrait aux cantons de décider la mise à disposition du formulaire sous format électronique, dans les cas où la loi exigeait l'utilisation d'un formulaire[115]. Le Conseil fédéral indiquait également qu'il appartiendrait à la pratique et à la jurisprudence de mettre en évidence les cas où le législateur parle de forme écrite sans exiger de signature manuscrite (*Textform* du droit allemand)[116].

Il convient de se montrer toutefois plus nuancé.

D'une part, dans un arrêt du 8 juillet 2003[117], le Tribunal fédéral a précisé que la formule officielle de hausse de loyer (et donc par analogie aussi pour les autres cas où la formule officielle est prescrite) se devait d'être signée de manière manuscrite, une simple reproduction mécanique de la signature (art. 14 al. 2 CO) étant insuffisante. Bien que cet arrêt soit critiqué par la doctrine[118], cette jurisprudence implique en l'état que la formule officielle soit signée. Le Tribunal fédéral utilise certes le terme de forme écrite « qualifiée » (*qualifizierte Schriftform*), mais la qualification ne vise que l'utilisation de la formule officielle en sus des autres exigences de la forme écrite simple (cf. supra II.2), soit l'exigence de l'écrit et de la signature manuscrite. Il s'agit d'une *condition de validité de l'acte*, mais non de la définition de la forme elle-même (cf. supra II.2.a).

D'autre part, les formulaires officiels sont dans la pratique reproduits sous forme de document électronique depuis longtemps par les professionnels de l'immobilier, afin de compléter les rubriques requises directement à l'écran et imprimer la formule remplie, sans avoir attendu que l'autorité mette cette possibilité à disposition. Le sens et le but de la formule officielle sont respectés (attirer l'attention de la partie faible et l'informer sur ses droits), dans la mesure où les formules officielles ainsi scannées ou reproduites comportent un texte et une mise en page

---

114 *Sans être exhaustif* : fixation délai comminatoire en cas de demeure (257d CO) ou en cas de violation du devoir de diligence (257f CO), fixation au bailleur d'un terme pour remédier aux défauts (259g CO), autorisation pour le locataire d'effectuer des travaux de rénovation (260a CO), transfert du bail commercial (263 CO), résiliation du bail par le locataire (266l al. 1 CO), demande de baisse de loyer du locataire (270a CO), motivation du congé (271a al. 2 CO).

115 Message du CF, FF 2001, p. 5427.

116 Ce cas n'est ainsi pas réglé par la loi, contrairement au droit allemand, Langer, Verträge mit Privatkunden im Internet, Zurich 2003, p. 234-235.

117 ATF 4C.110/2003 du 8 juillet 2003 = CdB 4/03, p. 97 ss.

118 Richard, Nécessité ou non de la signature par le bailleur, a fortiori autographe, de la formule de notification de hausse de loyer ou de nouvelles prétentions et de la formule de résiliation, in : CdB 01/04, p. 1 ss.

identiques à la formule originale. On peut toutefois imaginer que les autorités cantonales mettent effectivement à disposition un formulaire en ligne que l'on pourrait directement remplir puis imprimer et /ou sauvegarder sur son disque dur[119].

Même si dans ses considérants le Tribunal fédéral ne s'est pas prononcé sur l'admissibilité d'une signature manuscrite figurant dans une lettre d'accompagnement en annexe du formulaire officiel, cette question peut à notre sens demeurer ouverte en matière de signature électronique. En effet, ainsi qu'on l'a vu plus haut (II.3.c), la signature électronique constitue un ensemble de données numériques chiffrées, *distinctes du message original*. Le lien entre le texte et sa signature n'est donc plus physique, mais *logique*. Dès lors, la nature même de la signature électronique ne permet pas à celle-ci de figurer « sur » le formulaire officiel transmis par voie électronique. Dans la mesure où la signature électronique « scelle » le message dans lequel est contenu le formulaire officiel, les exigences posées par le Tribunal fédéral, soit que l'identité du déclarant soit clairement établie et que le contenu puisse être imputé à quelqu'un, sont remplies. En effet, la signature électronique qualifiée est expressément liée à une personne physique déterminée par le biais du certificat. L'imputabilité de la déclaration de volonté sur laquelle insiste le Tribunal fédéral est ainsi assurée.

Ainsi, contrairement à Probst[120], le principe d'une notification d'une formule officielle (congé, hausse, nouvelles prétentions, loyer initial) à l'aide de la signature électronique et par voie dématérialisée doit être admis à notre sens, l'équivalence de celle-ci avec la signature manuscrite étant désormais assurée.

3. Respect des termes et délais

Ce sujet a déjà été traité en détail par la doctrine[121] et il n'y est revenu que dans le cadre des relations dématérialisées.

La notification des actes en matière conventionnelle est, sauf exception, soumise au principe de la réception ; l'envoi est réputé notifié lorsqu'il se trouve dans la sphère d'influence du destinataire et que celui-ci est à même d'en prendre connaissance. Lorsque l'acte est formateur, c'est également la théorie de la réception qui s'applique.

En matière dématérialisée, on peut tirer les mêmes parallèles qu'avec le courrier postal simple et le courrier recommandé. Il s'agit avant tout d'une question de preuve.

Le Tribunal fédéral a retenu que dès qu'une lettre est entrée dans la sphère d'influence du destinataire, celui-ci assume le risque que, dans l'intérieur de cette sphère, la lettre ne parvienne pas à sa connaissance[122]. Il en va dès lors ainsi de même par l'intermédiaire d'Internet : la

---

119 C'est le cas depuis longtemps des formulaires utilisés dans le cadre de la LP.

120 Probst, Le droit du bail et Internet, in : 11e Séminaire sur le droit du bail, Neuchâtel 2000, p. 17.

121 Voir en particulier Bohnet, Les termes et délais en droit du bail à loyer, 13e Séminaire sur le droit du bail, Neuchâtel 2004, p. 4 s.

122 Bohnet, Les termes et délais en droit du bail à loyer, 13e Séminaire sur le droit du bail, Neuchâtel 2004, p. 6 et note 31.

notification doit ainsi être considérée comme réalisée dès qu'elle est entrée dans le système désigné par le destinataire, même si celui-ci est géré par un tiers[123].

Un simple *e-mail* correspond au courrier simple. L'expéditeur peut demander un accusé de réception (option de son logiciel de messagerie), sans être sûr que le destinataire consente à renvoyer cette confirmation. Il n'y a donc aucun moyen de prouver de manière certaine ni l'expédition, ni la réception.

Le courrier électronique qui passe en revanche par un tiers de confiance apposant un cachet postal électronique permet de remédier à la fois à la difficulté de la preuve du moment de l'expédition (« Preuve de l'envoi ») et du moment de la réception (« accusé de réception ») et du contenu de la communication (et ce, contrairement au courrier postal traditionnel, qui ne pose que des présomptions).

S'agissant des termes et délais judiciaires, nous relevons que depuis le 1er janvier 2007, certaines communications avec le Tribunal fédéral peuvent s'effectuer par voie électronique (cf. supra note 77) et ce système est amené à se développer aux trois échelons politiques de notre pays.

IV. Conclusion

La principale raison de la lenteur du décollage de la signature électronique est principalement sa complexité, difficile à cerner pour le néophyte. D'autre part, les fournisseurs de services ont été jusqu'ici peu incités à élaborer une signature électronique à usage multiple, exigeant une masse critique d'utilisateurs et d'applications. Ils ont longtemps préféré offrir des solutions « propriétaires » pour leurs services, comme par exemple le secteur des services financiers.

Cependant, le législateur a donné désormais l'impulsion nécessaire pour renforcer la confiance dans le e-commerce, geste attendu avec impatience par le monde économique en raison de l'essor de la dématérialisation des communications (il sera bientôt possible de conclure un contrat de bail via son téléphone mobile).

Dans le domaine particulier du droit du bail, les relations directes et personnelles entre les parties sont encore monnaie courante. Cet état de fait ne favorise dès lors guère le recours à des moyens de communication dématérialisés, à tout le moins pour la conclusion du contrat de bail.

Toutefois, il est certain que l'utilisation de la signature électronique se fera de manière de plus en plus fréquente, en particulier dans les communications des parties ultérieures à la conclusion du bail, dès lors que les services postaux officiels mettront à disposition un service d'horodatage efficace, facile à utiliser et d'un coût modéré.

---

123 Cherpillod Giacobino, Internet dans la conclusion du contrat et les solutions de paiement, SJ 2003 II, p. 393-434, p. 409 ; Jaccard, La formation des contrats sur Internet et la vente aux enchères en ligne, in : Quelques facettes du droit de l'Internet, volume 1, Neuchâtel 2001, p. 61 ; Probst, Le droit du bail et Internet, in : 11e Séminaire sur le droit du bail, Neuchâtel 2000, p. 13 et note 52 ; selon Briner (Verträge und Haftung im Internetrecht, Zurich 2002, p. 39) à mesure que le destinataire a désigné une adresse électronique, on peut attendre de lui qu'il relève régulièrement sa boîte aux lettres électronique, tout comme il est censé le faire avec son courrier postal traditionnel ; Donzallaz, La notification en droit interne suisse : étude de procédures civile, pénale et administrative cantonales et fédérales, Berne 2002, n° 665, p. 348.

Bibliographie

Becker Arnd	Elektronische Dokumente als Beweismittel im Zivilprozess, Frankfurt am Main 2004
Bohnet François	Les termes et délais en droit du bail à loyer, 13e Séminaire sur le droit du bail, Neuchâtel 2004
	La Théorie générale des papiers-valeurs, Thèse, Neuchâtel 2000
Briner Robert G.	Verträge und Haftung im Internetrecht, Zurich 2002
Cahen Muriel-Isabelle	La preuve sur Internet : Les règles classiques et l'apport de la signature électronique, 2003 (www.droit-ntic.com) http://www.droit-ntic.com/news/afficher.php?id=138
Cerrutti Davide	La protection de la partie faible et la loi sur la signature électronique, Bulletin Cedidac no 40, Novembre 2004, Lausanne
Cherpillod Giacobino Anne	Internet dans la conclusion du contrat et les solutions de paiement, in : SJ 2003 II 393 ss
Dilger Petra	Verbraucherschutz bei Vertragabschlüssen im Internet, München 2002
Donzallaz Yves	La notification en droit interne suisse, Berne 2002
Fanger Reto	Digitale Dokumente als Beweis im Zivilprozess, Bâle 2005
Favre-Bulle Xavier	Le Contrat électronique, in : Le contrat dans tous ses états, Berne 2004, p. 175 ss
Frei Oliver	Der Abschluss von Konsumentenverträgen im Internet, Zurich 2002

Gasser Urs / Häusermann Daniel M. / Müller Michael	E-mail im Wechselspiel von Informations technologie und Recht, in : www.swisslex.ch, 19 mai 2006
Ghernaouti-Hélie Solange	Sécurité Internet, Stratégies et technologies, Paris 2000
Ghernaouti-Hélie Solange / Dufour Arnaud	De l'Ordinateur à la société de l'information, Que Sais-Je n° 3541, 2e éd., PUF, Paris 2001
Hohl Fabienne	Le degré de la preuve dans les procès au fond, in : Der Beweis im Zivilprozess / La preuve dans le procès civil ; Fondation pour la formation continue des juges suisses, Berne 2000, p. 127 ss (Le degré de la preuve)
	Procédure civile, tomes I et II, Berne 2001 et 2002 (Procédure)
Jaccard Michel	Forme, preuve et signature électronique, in : Aspects juridiques du commerce électronique, Zurich 2001, p. 113 ss
	La formation des contrats sur Internet et la vente aux enchères en ligne, in : Quelques facettes du droit de l'Internet, volume 1, Neuchâtel 2001
	Le renforcement de la sécurité du droit par l'apport de la technologie: L'exemple de la signature électronique, in : DC 2002, p. 99 ss
	Le législateur suisse à l'épreuve d'Internet : aperçu de l'Avant-Projet de loi fédérale sur le commerce électronique in : SJ 2003 II 209 ss
Lachat David	Le bail à loyer, Lausanne 1997
Langer Dirk	Verträge mit Privatkunden im Internet, Zurich 2003
Lathoud Bertrand	La gestion formelle de la trace informatique : un moyen de renforcer la politique de sécurité d'un système d'information, Thèse, Lausanne 2002
Linant de Bellefonds Xavier	Pratique du droit de l'informatique, Logiciels - systèmes - Internet, Dalloz, Paris 2002

Montero Etienne	Du recommandé traditionnel au recommandé électronique : vers une sécurité et une force probante renforcée in : Le Commerce électronique : de la théorien à la pratique, Cahiers du CRID, n° 23, Bruxelles, Bruyant, 2003, p. 69-99
	L'ouverture de la preuve littérale aux écrits sous forme électronique, in : Journal des tribunaux, n° 6000 du 17 février 2001, p. 114 ss
Probst Thomas	Le droit du bail et Internet, 11e Séminaire sur le droit du bail, Neuchâtel 2000
Schlauri Simon	Elektronische Signaturen, thèse, Zurich 2002
Sédallian Valérie	La sécurisation des échanges électroniques, Eurostaf, Paris 2003
Spahr Christophe	Internet und Recht, Zurich, 2000, in : Internet Recht und Electronic Commerce Law
Spühler Karl	Behauptungslast und Beweiswürdigung bei hochtechnischen Zusammenhängen / Le fardeau de l'allégation et l'appréciation de la preuve dans des contextes hautement techniques, in : Der Beweis im Zivilprozess / La preuve dans le procès civil ; Fondation pour la formation continue des juges suisses, Berne 2000, p. 93 ss
Tercier Pierre	Les Contrats spéciaux, 3e éd, Zurich 2003

Message du Conseil fédéral du 3 juillet 2001 relatif à la loi fédérale sur les services de certification dans le domaine de la signature électronique	FF 2001, p. 5423 ss
Office fédéral de la Justice	Avant-projet de loi fédérale de procédure civile et rapport explicatif (juin 2003)