Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La preuve des actes juridiques privés électroniques en droit belge

Montero, Etienne

Published in:
Revue Lamy Droit de l'Immatériel

Publication date:
2009

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Montero, E 2009, 'La preuve des actes juridiques privés électroniques en droit belge', *Revue Lamy Droit de l'Immatériel*, numéro 52 supplément, pp. 19-26.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 02. May. 2026

C'est à une analyse du système de la preuve de la signature électronique dans le droit belge ainsi que du régime probatoire de la signature électronique dans son rapport avec celui de l'acte juridique à laquelle nous convie présentement Me Étienne Montero.

La preuve des actes juridiques privés électroniques en droit belge

Par Étienne MONTERO
Doyen de la Faculté de Droit de Namur (Académie universitaire Louvain)
Directeur de recherches au Centre de Recherches Informatique et Droit (CRID)

INTRODUCTION

La présente étude est centrée sur le régime de la signature électronique et ses rapports avec l'acte juridique privé. Avant d'entrer dans le vif du sujet, il n'est pas inutile de formuler une double observation (1).

Remarquons d'emblée que le régime juridique de la signature électronique est éclaté en une myriade de textes, ce qui complique singulièrement la matière. À vrai dire, la manière dont la directive 1999/93 sur les signatures électroniques (2) a été transposée en droit belge n'enchante guère sur le plan légistique. Initialement, deux textes avaient été préparés : un avant-projet de loi « *visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations* » (3) et un avant-projet de loi « *relatif à l'activité d'autorités de certification agréées en vue de l'utilisation de signatures digitales* » (4). Le premier texte n'a pu être adopté sous la législature qui l'a vu apparaître. Suite à divers avatars, ce texte – largement remanié et destiné à modifier les règles de preuve du Code civil – a refait surface sous la forme, pour le moins curieuse, d'un amendement à une proposition de loi tendant à modifier... le Code judiciaire (5). Cet amendement est à l'origine du nouvel alinéa 2 de l'article 1322 du Code civil relatif à la signature électronique. Le second texte, profondément remanié lui aussi (6), est devenu la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (7). Cette loi accorde un régime de faveur à la « *signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique* ». Pareille signature est assimilée de plein droit à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale (8). Pour le reste, comme l'indique son intitulé, la loi définit le régime juridique applicable aux activités des prestataires de service de certification (en abrégé, « PSC »), ainsi que les règles à respecter par ces derniers et par les titulaires de certificats (9).

À l'issue d'un parcours législatif particulièrement long et tortueux, on se retrouve avec pas moins de quatre déclinaisons de la signature électronique.

Tout d'abord, le Code civil contient désormais, en son article 1322, alinéa 2, une définition fonctionnelle de la signature électronique dont il résulte que « *peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte* ».

Ensuite, la loi du 9 juillet 2001 reproduit littéralement les définitions de la directive 1999/93. La « *signature électronique* » est définie comme « *une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification* » (10). Quant à la « *signature électronique avancée* », elle s'entend d'« *une donnée électronique, jointe ou liée logiquement à d'autres données électroniques servant de méthode d'authentification et satisfaisant aux exigences suivantes :*

a) être liée uniquement au signataire ;

b) permettre l'identification du signataire ;

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable » (11).

Enfin, l'article 4, § 4, de la loi du 9 juillet 2001 est libellé comme suit : « *Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et créée par un dispositif sécurisé de création de signature est assimilée à une signature manuscrite,* >

(1) La présente étude s'appuie, pour partie, sur certains de nos travaux antérieurs, en particulier : Montero É., L'introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique fonctionnaliste ?, Mélanges offerts à Marcel Fontaine, Bruxelles, Larcier, 2003, p. 179-210 ; Signature et contrat dans les environnements électroniques ouverts, *in* Les deuxièmes journées internationales du droit du commerce électronique, Actes du Colloque, Nice, 6-7 nov. 2003, Litec, 2005, p. 187-197. (2) Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, JOCE 19 janv. 2000, n° L 13, p. 12. (3) Doc. parl., Ch. repr., sess. ord., 1998-1999, n° 2141/1, p. 20. (4) Doc. parl., Ch. repr., sess. ord., 1999-2000, doc 50 0322/001, p. 44 et s. (5) Le projet ainsi amendé deviendra la loi du 20 octobre 2000 « *introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire* », M.B., 22 déc. 2000, p. 42698. (6) Voir Amendement n° 1 du Gouvernement (10 nov. 2000), Doc. parl., Ch. repr., sess. ord. 2000-2001, doc 50 0322/002. (7) Moniteur Belge (M.B.), 29 juill. 2001, p. 33070. (8) L. 9 juill. 2001, art. 4, § 4, précitée. (9) Pour une analyse détaillée de cette loi, voir Gobert D., Cadre juridique pour les signatures électroniques et les services de certification : analyse de la loi du 9 juillet 2001, *in* Montero É. (coord.), La preuve, Formation permanente CUP, vol. 54, mars 2002, p. 83-172. (10) L. 9 juill. 2001, art. 2, 1°. (11) L. 9 juill. 2001, art. 2, 2°.

qu'elle soit réalisée par une personne physique ou morale ». Pareille signature électronique est généralement baptisée « *signature électronique qualifiée* » par la doctrine belge.

On ajoutera que certaines législations particulières font référence à une forme encore différente de signature électronique. Par exemple, la loi sur le contrat de travail prévoit qu'« *un contrat de travail signé au moyen de la signature électronique créée par la carte d'identité électronique ou d'une signature électronique qui satisfait aux mêmes conditions de sécurité que celles présentées par la signature électronique créée par la carte d'identité électronique* est assimilé à un contrat de travail papier signé au moyen d'une signature manuscrite » (12). La carte d'identité électronique met en œuvre une signature numérique à double clé cryptographique, fondée sur la technologie RSA et une infrastructure à clé publique. Elle est censée répondre aux conditions de la signature électronique qualifiée et, dès lors, bénéficie *en principe* (13) du régime d'assimilation de plein droit à la signature manuscrite.

Ce point nous amène à notre seconde observation, qui est essentielle pour bien saisir le contexte de la certification en Belgique. Il a été décidé, en 2003, de remplacer progressivement la carte d'identité traditionnelle par une carte d'identité électronique de manière à parvenir à une diffusion complète de cette dernière pour la fin de l'année 2009 (14). Dans ces circonstances, on comprend qu'un seul prestataire de certification de signature électronique soit aujourd'hui actif en Belgique. Qui peut trouver un intérêt à offrir des produits de signature qualifiée si tout le monde en disposera prochainement *via* la carte d'identité électronique ?

Nous analyserons présentement le système de la preuve de la signature électronique dans le droit belge (I), puis le régime probatoire de la signature électronique dans son rapport avec celui de l'acte juridique (II).

I. – LE SYSTÈME DE LA PREUVE DE LA SIGNATURE ÉLECTRONIQUE EN DROIT BELGE

A. – Quelle différence entre signature électronique certifiée et non certifiée ?

On rappelera que la directive 1999/93 invitait les États membres à consacrer dans leur droit interne ce qu'on convient d'appeler un principe d'assimilation (art. 5, 1) et un principe de non-discrimination (art. 5, 2). Les signatures électroniques « *qualifiées* » (15) bénéficient du principe d'assimilation tandis que les signatures électroniques bénéficient seulement du principe de non-discrimination.

Cela signifie, plus précisément, qu'à la différence des autres procédés de signature électronique, la signature électronique qualifiée est assimilée de plein droit à la signature manuscrite (16). Pratiquement, il en résulte, à suivre des auteurs belges, que la signature électronique qualifiée est toujours recevable en justice (17) et se voit reconnaître la même force probante que celle accordée à la signature manuscrite (18). Encore s'empressent-ils généralement de préciser que la référence à la force probante de la signature représente un raccourci de langage car la signature ne saurait être envisagée indépendamment de l'écrit. Aussi, préfèrent-ils la formulation suivante : les données électroniques liées à une signature électronique qualifiée sont assimilées de plein droit à des données imprimées sur lesquelles est apposée une signature manuscrite (voir II, ci-après).

Conformément au principe de non-discrimination, toute autre signature électronique – qui ne remplit pas les conditions de l'article 4, § 4, de la loi du 9 juillet 2001 – ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif :

« – *que la signature se présente sous forme électronique, ou ;*
– *qu'elle ne repose pas sur un certificat qualifié, ou ;*
– *qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou ;*
– *qu'elle n'est pas créée par un dispositif sécurisé de création de signature* » (19).

Cette disposition devrait permettre de rattraper divers procédés de signature électronique qui, pour l'une ou l'autre raison, ne peuvent bénéficier du régime d'assimilation automatique à la signature manuscrite. L'on songe à des procédés de signature électronique ordinaire : l'utilisation combinée d'un nom d'utilisateur et d'un mot de passe, un simple e-mail (qui contiendrait, par exemple, des données très personnelles à son auteur apparent), un bon de commande complété et envoyé directement sur le web (avec indication d'un code d'identification « client » ou de diverses données telles que le nom, l'adresse géographique et électronique, un numéro de carte de crédit...) (20), etc. On songe encore, notamment, à des signatures électroniques avancées non certifiées (21) ou réalisées sur la base d'un certificat non qualifié ou conçues au moyen d'un dispositif insuffisamment sécurisé de création de signature. Profitant de la marge de manœuvre qui lui est reconnue (voir ci-après), le juge pourrait se montrer plutôt accueillant – surtout dans un premier temps – en ce qui concerne ces divers procédés de signature, en dépit de leur fiabilité relative. Ainsi, il serait excessif de dénier toute efficacité juridique à une signature numérique à double clé cryptographique ordinaire pour le seul motif qu'elle n'a pas été créée par un dispositif sécurisé (22). Le juge pourrait reconnaître la qualité de signature à des mécanismes peu sécurisés, mais qui, à son estime, permettent d'établir avec une *fiabilité suffisante* les fonctions attendues de la signature.

Afin de dégager plus finement les différences entre le régime juridique de la signature électronique qualifiée et celui des autres procédés de signature électronique, je distinguerai deux ordres de considérations. On rappelera que dans le cadre du droit civil de la preuve, le juge ne peut soulever d'office une contestation : il ne peut vérifier d'initiative la validité d'une signature si les parties ne l'y invitent pas dans leurs conclusions. Force est de constater qu'il n'est pas courant que la signature manuscrite fasse l'objet d'une contestation. Mais cela arrive

---

(12) L. 3 juill. 1978 relative aux contrats de travail, art. 3 *bis*, al. 1er. **(13)** En réalité, la question est actuellement controversée. **(14)** Voir loi du 25 mars 2003 modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, M.B., 28 mars 2003, p. 15921 ; Arrêté royal du 25 mars 2003 relatif aux cartes d'identité, M.B., 28 mars 2003, p. 15929. **(15)** Pour rappel, il convient d'entendre par signature électronique qualifiée la « *signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique* ». **(16)** L. 9 juill. 2001, art. 4, § 4. **(17)** Rappelons que la *recevabilité* est la « *prise en considération, par le juge, d'éléments probatoires déclarés admissibles par la loi eu égard à l'objet du litige* ». Autrement dit, lorsqu'un élément de preuve est recevable, le juge est tenu de l'examiner, quitte à ne lui reconnaître aucune valeur probatoire. À l'inverse, la preuve irrecevable doit être écartée d'office par le juge, sans qu'il puisse en examiner la portée. **(18)** La force probante d'un acte est l'intensité quant à la preuve que la loi lui reconnaît et qui s'impose au juge : voir Cass., 21 juin 1999, Bull., 1999, n° 378, p. 930 (définition figurant dans le sommaire). Rappr. Dumon F., De la motivation des jugements et arrêts et de la foi due aux actes, J.T., 1978, p. 486. La notion renvoie à une certaine hiérarchie des modes de preuve. **(19)** L. 9 juill. 2001, art. 4, § 5. **(20)** Voir Lecocq L. et Vanbrabant B., La preuve du contrat conclu par voie électronique, *in* Le commerce électronique : un nouveau mode de contracter ?, Liège, Éditions du Jeune Barreau, 2001, p. 51-137, spéc. p. 117-118, nos 102 et 103. **(21)** Par ex., des signatures numériques fondées sur PGP (*Pretty Good Privacy*). Téléchargeable gratuitement sur l'internet, ce programme permet à tout internaute de générer une paire de clés et de diffuser lui-même sa clé publique (chaque utilisateur dispose de toute une collection de clés publiques réunies dans un fichier appelé « *trousseau de clés publiques* »). PGP n'a pas techniquement besoin de l'intervention d'une autorité de certification pour être exploité ; voir Bitan H., La signature électronique : comment la technique répond-elle aux exigences de la loi ?, Gaz. Pal., 2000, p. 1280. **(22)** C'est-à-dire qui satisfait à toutes les exigences de l'annexe III de la loi du 9 juillet 2001.

parfois. Pratiquement, le débat judiciaire peut tourner autour de deux questions distinctes (23). Une première question concerne la *validité* du procédé de signature utilisé. En cas de signature valable, une seconde question peut surgir : cette signature est-elle *imputable* au signataire apparent ? Il est encore loisible à ce dernier de désavouer son écriture, auquel cas, selon le contexte, le signataire apparent peut soit inciter le demandeur à recourir à la procédure de vérification d'écritures, soit engager une procédure d'inscription de faux. La signature électronique peut donner lieu au même double débat.

1°/ La validité de la signature

Tout d'abord, le juge peut être invité à se prononcer sur la validité d'une signature.

En matière de signature traditionnelle, ce simple problème juridique de qualification peut être aisément tranché par le juge. Ainsi, peut-il estimer que tel signe ne constitue pas une signature valable pour divers motifs : soit le signe est illisible, soit il n'a pas été apposé directement sur le document (24) mais par le truchement d'un papier carbone, d'une photocopie ou d'une télécopie... ; soit il ne manifeste pas l'adhésion de son auteur au contenu de l'acte (eu égard à son emplacement... (25)).

Le débat portant sur la validité d'une signature électronique non qualifiée – qu'elle soit ordinaire ou avancée – conduit à des vérifications plus *complexes* et *subjectives*.

Le même type de contestation peut s'élever à propos d'une signature électronique. C'est ici que s'apprécie tout l'intérêt de recourir à la signature électronique qualifiée. En effet, cette dernière étant assimilée automatiquement à une signature manuscrite, « *le juge n'est dès lors pas tenu de procéder à d'autres vérifications que celles qu'il effectuerait en présence d'une signature manuscrite* » (26). Ces deux types de signatures se présentant naturellement sous des dehors différents, les vérifications qui s'imposent ne sont pas comparables pratiquement. Toutefois, il est vrai que, dans le cas de la signature électronique qualifiée, elles seront aussi *simples* et *objectives* qu'en matière de signature manuscrite. Si la signature électronique est certifiée par un prestataire accrédité, le juge pourra se borner à constater cette accréditation (laquelle suppose le respect des exigences des annexes I, II et III de la loi du 9 juillet 2001). Si la signature est délivrée par une autorité de certification non accréditée, le respect des exigences énoncées dans les trois annexes de la loi devrait être démontré. Toutefois, en pratique, les vérifications à effectuer restent relativement aisées : il suffira au juge de vérifier que le certificat est qualifié et de demander une attestation à l'administration chargée de contrôler ces prestataires (27).

En revanche, le débat portant sur la validité d'une signature électronique non qualifiée – qu'elle soit ordinaire ou avancée (28) – conduit à des vérifications plus *complexes* et *subjectives*. En effet, dans le cadre de la preuve d'un acte juridique privé, le juge devra vérifier, en cas de contestation, si le procédé de signature électronique qui lui est présenté satisfait aux conditions d'imputabilité et d'intégrité posées par l'article 1322, alinéa 2, du Code civil. Pratiquement, il lui revient d'apprécier l'aptitude du procédé à identifier le signataire, à attester son adhésion au contenu de l'acte et à garantir le maintien de l'intégrité du contenu de l'acte (29). Il jouit, à cet égard, d'un incontestable pouvoir d'appréciation quant au degré de fiabilité dont il se satisfait. Pourvu qu'il motive sa décision de façon cohérente, eu égard aux conditions de l'article 1322, alinéa 2, on conviendra que sa marge de manœuvre est appréciable à l'heure de considérer si le procédé de signature électronique est valable ou non. En pratique, la signature manuscrite réserve normalement peu de surprise : pourvu qu'elle consiste en la marque habituelle du signataire et qu'elle soit tracée au bon endroit, sa validité est assurée. Sauf rares exceptions (la griffe, les empreintes digitales, la signature à main guidée...), on n'a jamais eu à se préoccuper de la fiabilité de la signature sur papier, ni du procédé utilisé. Du reste, le juge peut trancher seul et aisément la question de la qualification.

Les signatures électroniques sont nettement plus imprévisibles. Les questions relatives au procédé utilisé et à sa fiabilité deviennent ici essentielles. Hors la signature électronique qualifiée, l'on a vu qu'en cas de contestation, il revient au juge d'apprécier l'aptitude du procédé à établir l'imputabilité et le maintien de l'intégrité. La grande latitude laissée au juge entraîne une insécurité juridique, qui est, sinon nulle, pratiquement négligeable en présence d'une signature traditionnelle... ou d'une signature électronique qualifiée. En outre, il devra souvent faire appel à un expert pour évaluer la validité d'un procédé de signature électronique qui ne répond pas aux critères de la signature qualifiée. On devine les inconvénients qui s'ensuivent en termes de coût et d'allongement des procédures.

2°/ L'imputabilité de la signature

Sans contester la validité du mécanisme de signature électronique, le défendeur peut-il encore affirmer ne pas avoir signé ? L'auteur présumé d'une signature électronique non qualifiée a incontestablement le loisir de dénier sa signature, obligeant ainsi le demandeur a recourir éventuellement à une vérification d'écritures (30). Cette solution ressort explicitement des travaux préparatoires relatifs à l'article 1322, alinéa 2, du Code civil (31). Selon une opinion, « *cette vérification d'écritures* se confondra *le plus souvent avec l'opération consistant à vérifier l'imputabilité de l'acte. En vidant, éventuellement, au terme d'une expertise, la question si le message qui lui est soumis est bien imputable à l'une des parties au procès, le juge aura* ipso facto *procédé à une vérification d'écritures* » (32). Selon une autre opinion, la question de la validité de la signature doit se résoudre *in abstracto* (le procédé présenté est-il en soi suffisamment fiable pour permettre d'identifier telle personne ?), tandis que la vérification d'écriture à proprement parler suppose une vérification *in concreto* (dans le cas d'espèce, est-ce bien le prétendu signataire qui a utilisé le procédé ?) (33). Dans cette optique, l'on peut penser

---

(23) À cet égard, voir D. Mougenot, La preuve, 3e éd., Bruxelles, Larcier, 2002, p. 225, n° 158-1 ; égal. Montero É., L'introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique fonctionnaliste ?, précité, spéc. p. 194 et s. **(24)** Il résulte de la jurisprudence de la Cour de cassation que « *la signature d'un acte sous seing privé doit, en règle, être tracée directement sur le document lui-même* » (Cass., 28 juin 1982, Pas., 1982, I, p. 1286, R.C.J.B., 1985, p. 57 et s., et la note de M. Van Quickenborne, Quelques réflexions sur la signature des actes sous seing privé). **(25)** Voir Verheyden-Jeanmart N., Droit de la preuve, Bruxelles, Larcier, p. 240-241. **(26)** Projet de loi relatif à la procédure par voie électronique, Commentaire des articles, Doc. parl., Ch. repr., sess. ord. 2004-2005, n° 1701/001, 11 avr. 2005, p. 16. **(27)** En ce sens, Lecocq L. et Vanbrabant B., précité, p. 119-121, nos 106 et 107; Storme M.E., *De invoering van de elektronische handtekening in ons bewijsrecht – Een inkadering van en commentaar bij de nieuwe wetsbepalingen*, R.W., 2000-2001, p. 1519, n° 45 ; Guinotte L., La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001, J.T., 2002, p. 558. **(28)** L. 9 juill. 2001, art. 2, 1° et 2°. **(29)** À ce sujet, pour plus de précisions, voir il, ci-après. **(30)** Sur cette procédure, Rouard P., Traité élémentaire de droit judiciaire privé, t. IV, Bruxelles, Bruylant, 1980, p. 37 et s., nos 33 et s. ; égal., Fettweis A., Manuel de procédure civile, 2e éd., Faculté de droit de Liège, 1987, p. 362, n° 485. **(31)** Voir Justification de l'amendement n° 12 (du Gouvernement) à la Proposition de loi introduisant de nouveaux moyens de télécommunication dans la procédure judiciaire et extrajudiciaire (13 juin 2000), Doc. parl., Ch. repr., sess. ord., 1999-2000, n° 0038/006, p. 12 ; voir aussi le rapport fait au nom de la Commission de la justice par Bart Somers (30 juin 2000), Doc. parl., Ch. repr., sess. ord., 1999-2000, n° 0038/008, p. 33, ainsi que l'avis du Conseil d'État sur le premier projet preuve : Doc. parl., Ch. repr., sess. ord., 1998-1999, 2141/1, p. 28. **(32)** Lecocq P. et Vanbrabant B., précité, p. 116, n° 100. **(33)** Mougenot D., La preuve, précité, p. 225, n° 158-1.

qu'avec le temps et l'expérience – et la constitution progressive d'un *corpus* jurisprudentiel –, le juge pourra trancher (parfois ? souvent ?) la question de la validité sans expertise, auquel cas la vérification d'écritures retrouvera un intérêt spécifique.

Par contre, la possibilité de dénier une signature électronique qualifiée fait débat dans la doctrine belge (34). Étant donné la haute fiabilité de pareille signature – et, partant, le faible risque de fraude –, une partie de la doctrine considère qu'elle ne peut être contestée (35). Pour notre part, nous pensons que l'auteur présumé d'une signature électronique qualifiée peut également dénier sa signature et obliger le demandeur à recourir éventuellement à une procédure de vérification d'écritures. D'une part, l'article 4, § 4, *initio*, de la loi du 9 juillet 2001 réserve expressément la possibilité de désavouer une signature électronique qualifiée. D'autre part, la solution contraire signifierait un alignement du régime probatoire de l'acte sous seing privé électronique sur celui de l'acte authentique traditionnel.

Faut-il le rappeler ? La différence fondamentale entre l'acte sous seing privé et l'acte authentique réside en ce que le premier est dépourvu de toute force probante quant à son origine – il ne prouve rien, il ne constitue pas une preuve – *tant qu'il n'est pas reconnu ou légalement tenu pour tel* (C. civ., art. 1322, al. 1er). Celui auquel on oppose un acte sous seing privé peut donc toujours se borner à désavouer son écriture ou sa signature (C. civ., art. 1323), ou, si l'acte émane d'un de ses auteurs, à déclarer qu'il ne connaît pas la signature. En toute hypothèse, une dénégation pure et simple suffit pour qu'aucune foi ne s'attache à un acte sous seing privé. Il incombe alors à celui qui invoque l'acte d'en rétablir la force probante en prouvant l'authenticité de la signature, au besoin par le recours à une demande en vérification d'écritures. L'acte authentique, au contraire, ne doit pas être reconnu : parce qu'il a fait l'objet de constatations par un officier public, il jouit d'emblée d'une force probante provisoire : l'origine de l'écriture et tout ce qui a été constaté *ex propriis sensibus* par l'officier public est susceptible de preuve contraire, mais par la seule voie de l'inscription de faux (36).

Le refus de la possibilité de désavouer une signature électronique certifiée entraînerait un bouleversement du droit de la preuve – perspective que les promoteurs de la réforme n'ont précisément pas voulue ! (37) – et serait en contradiction flagrante avec la philosophie qui est à la base de la réforme et la logique fonctionnaliste qui préside à celle-ci (38). En effet, contrairement à ce qui a toujours été proclamé (39), il n'y aurait donc pas *équivalence* entre la signature électronique qualifiée et la signature manuscrite, mais *supériorité* de la première sur la seconde ! Pour le dire autrement, nonobstant la terminologie employée à l'article 4, § 4, de la loi du 9 juillet 2001, il n'y aurait pas *assimilation* de l'acte sous seing privé électronique à l'acte sous seing privé traditionnel (sur support papier), mais *supériorité* du premier sur le second (40). Cela étant, il ne faudrait pas grossir le risque de dénégations abusives de signature électronique qualifiée (41).

Encore le débat pourrait-il se déplacer sur le terrain des responsabilités... et venir tempérer l'effet du désaveu. C'est ici qu'apparaît une autre différence – de taille ! – entre la signature manuscrite et la signature électronique. Jusqu'ici, le seul risque de fraude était l'imitation de signature. Or, on voit mal comment on aurait pu reprocher une faute dans le chef du prétendu signataire et le tenir pour responsable des conséquences de la fraude.

En matière de signature numérique, la fraude la plus vraisemblable est l'hypothèse de l'usurpation de clé privée. Dans une telle hypothèse, une négligence du signataire apparent n'est pas à exclure dès lors qu'il est « *seul responsable de la confidentialité* » de sa clé privée et tenu, en cas de doute quant à cette confidentialité, de faire révoquer le certificat (42). Dans ce cas, si le désaveu de signature conduit à écarter des débats l'acte invoqué, le demandeur peut encore chercher à mettre en cause la responsabilité aquilienne du signataire. Ce dernier devra répondre, le cas échéant, des ruptures de confidentialité de sa clé privée. Ainsi, le débat relatif à l'imputabilité de l'écriture et de la signature à son auteur prétendu pourra se poursuivre sur le terrain de la responsabilité. Question inédite sous l'empire de la signature traditionnelle et qui confère une tournure nouvelle à la question du désaveu de signature ! Le débat sur la preuve glisse largement vers un débat sur la sécurité, la gestion du risque et l'imputabilité de la responsabilité.

> En matière de signature numérique, la fraude la plus vraisemblable est l'hypothèse de l'usurpation de clé privée.

B. – L'organisation de la certification de signature

Le régime juridique de la certification est précisé par deux textes : d'une part, la loi du 9 juillet 2001 et ses annexes, d'autre part, l'arrêté royal du 6 décembre 2002 organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés (43) (soit « *certifiés* » dans le cade de la présente étude).

1°/ Comment faire certifier une signature électronique ?

Pour faire certifier une signature électronique, il y a lieu de s'adresser à un prestataire de service de certification (« PSC »). Préalablement à la délivrance d'un certificat, celui-ci vérifie non seulement la complémentarité des données afférentes à la création et à la vérification de signature (44), mais aussi l'identité (45) et, le cas échéant, les qualités spécifiques (un titre,

---

(34) Pour un exposé de la controverse, voir Montero É., L'introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique fonctionnaliste ?, précité, p. 199, n° 13. **(35)** Voir par ex., Storme M.E., *De invoering van de elektronische handtekening in ons bewijsrecht – Een inkadering van en commentaar bij de nieuwe wetsbepalingen*, R.W., 2000-2001, p. 1505-1525, spéc. p. 1519, n° 46, *initio* ; Dumortier J. et Van den Eynde S., *De juridische erkenning van de elektronische handtekening, Computerr.*, 2001, p. 185 et s., spéc. p. 193 et note 44. **(36)** Pour le reste, les deux types d'actes sont pratiquement sur le même pied. L'acte sous seing privé reconnu (ou tenu pour tel) « *a la même foi* » que l'acte authentique (art. 1322, al. 1er) : ils prouvent, dans la même mesure, la sincérité du *negotium* constaté et ils sont l'un et l'autre susceptibles de preuve contraire. Seul le mode d'administration de cette preuve diffère. Dans l'acte authentique, les mentions couvertes par l'authenticité ne peuvent être contredites, par une partie ou par un tiers, que par le biais de la procédure d'inscription de faux. Sous cette réserve, la sincérité des déclarations des parties, dans les deux types d'actes, peut être combattue par tous les moyens légaux, à savoir, inter partes, dans le respect de l'article 1341 du Code civil, et par les tiers, par toutes voies de droit (témoignages, présomptions...). À ce sujet, De Page H., Traité élémentaire de droit civil belge, t. III, Bruxelles, Bruylant, 1967, spéc. n° 747 ; Verheyden-Jeanmart N., Droit de la preuve, Bruxelles, Larcier, 1991, p. 271 ; Mougenot D., La preuve, précité, p. 221-222, n° 153. **(37)** Voir l'exposé des motifs du premier projet preuve, Doc. parl., Ch. repr., sess. ord., 1998-1999, 2141/1, spéc. p. 1 (« (...) *sans cependant réformer fondamentalement les principes essentiels de notre droit de la preuve* ») et p. 14 (« (...) *il convient de repenser nos règles juridiques en matière probatoire de façon à ce que, tout en maintenant l'équilibre des intérêts qu'elles entendaient assurer, elles ne constituent pas un obstacle au développement des nouvelles technologies* »). **(38)** Voir précité, spéc. p. 14-15 : « *Tout en maintenant le principe de la légalité des preuves et la prééminence de l'écrit consacrée à l'article 1341 du Code civil, il convient plutôt, par une analyse fonctionnelle des concepts d'écrit, de signature et d'original, de repenser les règles existantes de façon à les ouvrir aux moyens de preuve issus des nouvelles technologies de l'information* ». **(39)** Voir encore, par ex., Doc. parl., Ch. repr., sess. ord., 1999-2000, doc 50 0038/006, p. 2. **(40)** Rappr., *mutatis mutandis*, Devèze J., Vive l'article 1322 ! Commentaire critique de l'article 1316-4 du Code civil, *in* Le droit privé français à la fin du XXe siècle – Études offertes à Pierre Catala, Paris, Litec, 2001, p. 541. **(41)** Pour un plus ample développement, voir Montero É., L'introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique « fonctionnaliste », précité, spéc. p. 202-204, n° 15 ; Roger France E. et De Groote E., La valeur probante des signatures électroniques, R.D.C., 2002/3, spéc. p. 200. **(42)** L. 9 juill. 2001, art. 19, § 1er et 2. **(43)** M.B., 17 janv. 2003, p. 1541. **(44)** L. 9 juill. 2001, art. 8, § 1er. **(45)** À cet effet, le PSC peut s'adjoindre l'aide d'autorités dites d'enregistrement : communes (municipalités), chambres de commerce, ordres professionnels...

une fonction, un pouvoir...) de la personne qui en fait la demande (46). Le PSC fournit un exemplaire du certificat au candidat titulaire et conserve les certificats délivrés et le moment de leur expiration dans un annuaire (47). Les certificats qualifiés doivent satisfaire aux exigences visées à l'annexe I de la loi. On rappelera que les annexes I, II et III de la loi reproduisent en tous points les annexes de la directive 1999/93.

2°/ Le contrôle des PSC

Faisant écho au principe de non-autorisation préalable consacré par la directive sur le commerce électronique (48), il est rappelé à l'article 4, § 2, alinéa 1er, de la loi du 9 juillet 2001 que « *nul prestataire de service de certification ne peut être contraint de demander une autorisation préalable pour exercer ses activités* ». Néanmoins, est-il aussitôt précisé que les PSC qui entendent délivrer des certificats qualifiés ont l'obligation de se déclarer auprès de l'administration du ministère des Affaires économiques avant le début de leurs activités et de communiquer à cette dernière une série d'informations énumérées dans la loi : nom, adresse géographique d'établissement, coordonnées de contact, etc. (art. 4, § 2, al. 2). Cette administration est chargée, d'une part, des tâches relatives à l'accréditation éventuelle d'un PSC (49), d'autre part, de contrôler les PSC délivrant des certificats qualifiés au public et établis en Belgique (50).

Dès l'instant où un PSC qui délivre des certificats qualifiés s'est déclaré auprès de l'administration, celle-ci peut, à tout moment, prendre l'initiative d'un contrôle inopiné chez lui. Ce contrôle porte sur le respect des exigences des annexes I et II (51). À cet effet, elle peut faire appel aux services d'un ou de plusieurs experts afin de l'aider dans sa mission de contrôle. Ceux-ci doivent naturellement être indépendants, financièrement et administrativement, par rapport aux PSC. Les dépenses relatives aux contrôles sont à charge du ministère des Affaires économiques (52).

Une accréditation peut être demandée par tout PSC qui répond aux exigences des annexes II, délivre des certificats qualifiés satisfaisant aux exigences de l'annexe I et utilise des dispositifs de création de signature électronique conformes aux exigences de l'annexe III de la loi du 9 juillet 2001 (53). Cette accréditation se base sur le résultat d'un audit réalisé, aux frais du candidat, par une *entité* chargée d'évaluer le respect des exigences des annexes I, II et III. Cette entité est un organisme apte à démontrer sa compétence sur base d'un certificat délivré par le système belge d'accréditation conformément à la loi du 20 juillet 1990 concernant l'accréditation des organismes de certification et de contrôle, ainsi que des laboratoires d'essais, ou par un organisme équivalent établi dans l'Espace économique européen (54). Le PSC choisit librement parmi les entités celle qui sera chargée de son évaluation et informe l'administration de son choix. Cette dernière peut participer comme observateur aux audits d'évaluation des PSC, en étroite collaboration avec les entités. Au terme de son travail, l'entité remet un rapport d'évaluation et une attestation d'audit à l'administration. Si tous les éléments du rapport sont positifs, l'administration octroie une accréditation pour une durée de trois ans, renouvelable sur base de nouveaux rapports d'audit positifs (55).

Qu'en est-il dans les faits ? Comme il a été suggéré au début du présent exposé, la généralisation prochaine de la carte d'identité électronique – apte à remplir une fonction de signature électronique assimilée de plein droit à la signature manuscrite – a dissuadé les amateurs d'offrir des produits de signature qualifiée. Un seul PSC délivrant des certificats qualifiés est aujourd'hui déclaré en Belgique, Certipost, qui offre trois produits : *eTrust* (qui est le produit commercial : pour les notaires, même si la carte REAL est venue prendre le marché, pour les entreprises, déclarations DIMONA, etc.), *Citizen CA* (il s'agit de la carte d'identité électronique délivrée aux citoyens belges) et *Foreigner CA* (la carte d'identité électronique délivrée aux étrangers). Auparavant, Belgacom eTrust et Globalsign étaient également déclarés, mais ils ont cessé leurs activités, si bien que depuis 2006, seul Certipost reste en lice (56).

Il n'existe aucun PSC accrédité en Belgique. Aucune société n'en a jamais fait la demande, ce qui étonne dans le cas de Certipost, étant donné que la loi relative à la carte d'identité électronique prévoit que le PSC désigné doit être accrédité (57). Précisons que Certipost a été désigné par le Conseil des ministres et est lié par contrat à l'État belge. La production, la personnalisation et l'initialisation de la carte d'identité sont assurées par une société de droit privé, la société Zetes, qui a été désignée et est liée par contrat de la même façon que Certipost.

À ce jour, il n'existe pas encore d'application de signature des personnes morales. La nécessité d'une gestion souple et rapide des certificats, en raison des changements fréquents de fonctions au sein de la personne morale, représenterait un obstacle à l'attrait de pareille forme de signature.

Il va sans dire qu'il n'existe aucune entité au sens vu précédemment puisqu'il n'y a aucun candidat à l'accréditation. En revanche, des contrôles ont été opérés chez Globalsign, Certipost e-trust et Certipost eID, pour le compte et aux frais de l'administration, par certaines sociétés sélectionnées *via* un marché public (58).

3°/ Le rôle des normes réglementaires et techniques

Par référence à quelles normes réglementaires et techniques les contrôles sont-ils réalisés ?

L'arrêté royal qui organise le contrôle et l'accréditation des PSC qui délivrent des certificats qualifiés a créé un Comité technique auprès du ministère des Affaires économiques, composé d'un ou de plusieurs représentants du ministère des Affaires économiques, des PSC, des entreprises concernées les plus représentatives et des organisations de consommateurs les plus représentatives (59). Ce Comité est chargé, notamment, de l'élaboration et de l'approbation du « *référentiel d'accréditation* », défini comme un document de référence détaillant les moyens techniques pouvant être mis en œuvre pour être conforme aux critères d'accréditation (60), et des « *lignes directrices relatives à l'accréditation* », qui s'entendent des documents de référence utilisés lors des audits pour déterminer la façon dont la conformité aux critères d'accréditation peut être démontrée (61), de l'approbation et du contrôle de la liste des entités et de l'instruction des recours et plaintes introduits par des PSC.

En réalité, seule une version de « *référentiel d'accréditation* » de 400 pages a été mis au point en février 2005 mais, d'une part, il n'a jamais été approuvé par le Comité technique, en sommeil (62), d'autre part, il doit être sérieusement remis à jour (un appel d'offres est en préparation, en vue d'une mise à jour – prochaine – du référentiel).

(46) L. 9 juill. 2001, art. 8, § 2. **(47)** L. 9 juill. 2001, art. 9 et 10. **(48)** Voir l'article 4 et le considérant n° 28 de la directive sur le commerce électronique. **(49)** L. 9 juill. 2001, art. 17, § 1er, et 18. **(50)** L. 9 juill. 2001, art. 20. **(51)** L. 9 juill. 2001, art. 11. **(52)** Sur tout ceci, voir l'article 7 de l'arrêté royal du 6 décembre 2002, précité. **(53)** L. 9 juill. 2001, art. 17, § 1er, al. 2. **(54)** L. 9 juill. 2001, art. 2, 13°. **(55)** Voir l'article 4 de l'arrêté royal du 6 décembre 2002, précité. **(56)** Signalons, pour être complet, qu'une société, appelée Isabel, offre un produit de signature électronique fondée sur un certificat qualifié, mais uniquement dans le cadre d'un réseau fermé (des banques et des entreprises) et non pas pour le grand public. Par conséquent, ce PSC n'est ni déclaré, ni contrôlé. La signature électronique est assimilée conventionnellement à la signature manuscrite. **(57)** Voir l'article 14 de la loi du 25 mars 2003, précitée. **(58)** ICT Control, Price Waterhouse Coopers... **(59)** Pour plus de précisions, voir l'article 5 de l'arrêté royal du 6 décembre 2002, précité. **(60)** Article 1er, 7°, de l'arrêté royal du 6 décembre 2002, précité. Les « critères d'accréditation » désignent essentiellement les exigences figurant dans l'article 17, § 1er, de la loi du 9 juillet 2001, qui renvoient aux annexes I, II et III. **(61)** Article 1er, 8°, de l'arrêté royal du 6 décembre 2002, précité. **(62)** Depuis sa création, le Comité technique s'est réuni seulement deux fois, sans le *quorum* requis, et n'a jamais vraiment été opérationnel, faute de moyens.

En pratique, ce document sert de lignes directrices pour l'évaluation des PSC déclarés, même s'il est beaucoup plus détaillé que de simples lignes directrices. Il est communiqué (officieusement) aux intéressés et est utilisé pour le contrôle (sans qu'il soit nécessaire de contrôler au regard de tous les critères puisqu'il n'est pas question d'accréditation). Le PSC peut, semble-t-il, s'en éloigner s'il démontre qu'il atteint les mêmes objectifs par d'autres moyens. Le contrôle s'opère sur la base d'un *self-assessment* (auto-contrôle) : le prestataire met lui-même en avant les points sur lesquels il s'estime en conformité ou non avec les lignes directrices et l'administration opère des contrôles ponctuels sur certains de ces points.

Le référentiel technique mis au point s'inspire des trois normes reconnues par la Décision de la Commission du 14 juillet 2003 relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques conformément à la directive 1999/93/CE du Parlement européen et du Conseil (63). Des discussions sont en cours en vue d'adapter cette liste, estimée trop restrictive.

II. – LE RÉGIME PROBATOIRE DE LA SIGNATURE ÉLECTRONIQUE DANS SON RAPPORT AVEC CELUI DE L'ACTE JURIDIQUE

Force est de constater qu'avant l'avènement de la signature électronique, la notion de signature (manuscrite) retenait peu la doctrine. Qui plus est, les rares développements qui lui aient jamais été consacrés sont dus presqu'exclusivement à la doctrine civiliste (64). Apparemment, la signature est à ranger au nombre de ces notions – le nom, le domicile, l'état... – qui s'imposent en toute matière, nonobstant la circonstance que leur régime juridique a son siège principal dans le Code civil. Comme l'écrit Jean Carbonnier, « *C'est le droit civil qui a les clefs de l'individualisation de la personne, et les conclusions qu'il en tire pour lui-même ont une portée générale. Elles valent, en principe, pour l'ensemble du droit* » (65). La notion civiliste de signature – procédé d'identification s'il en est – rayonne pareillement au-delà du seul droit civil : en toutes matières, l'exigence d'une signature s'entendait, et s'entend toujours, au sens reçu par la notion en droit civil.

Or, en cette matière, la signature se rapporte toujours à un acte juridique. Il est traditionnellement enseigné que la signature remplit une double fonction : elle permet l'identification de son auteur et manifeste son adhésion au contenu de l'acte. En d'autres termes, la signature (reconnue ou non contestée) crée une présomption *juris et de jure* que le signataire a donné son consentement au contenu de l'acte signé par lui (66).

Certes, une signature se conçoit indépendamment d'un acte (authentique ou sous seing privé). On songe à une signature apposée sur une œuvre d'art, tel un tableau, ou sur un billet de banque. Mais c'est l'exception (67) car, en règle générale, la signature au sens juridique de la notion se rapporte toujours à un acte juridique. Le (rare) contentieux relatif à la signature – essentiellement en matière de testament holographe – renvoie invariablement à celui de l'acte lui-même. Il en résulte que la (maigre) réflexion doctrinale sur la preuve de la signature ne se dissocie guère de celle relative à la preuve de l'acte juridique lui-même. Ces considérations demeurent-elles pertinentes sur le terrain de la signature électronique ? C'est ce qu'il convient à présent d'examiner.

A. – Le régime de la preuve de la signature électronique est-il dissociable de celui de la preuve de l'acte juridique ?

Manifestement, la définition fonctionnelle de la signature électronique inscrite à l'article 1322, alinéa 2, du Code civil conçoit l'identification d'une personne dans ses rapports avec un document dont elle s'approprie le contenu. Il ressort, en effet, des travaux préparatoires de la loi du 20 octobre 2000 que la condition d'*imputabilité* est censée recouvrir les fonctions classiquement dévolues à la signature, à savoir l'*identification* (du signataire) et la manifestation de son *adhésion au contenu* de l'acte (68). Incidemment, on peut regretter que les fonctions d'identification et d'adhésion n'aient pas été expressément mentionnées à l'article 1322, alinéa 2. L'intérêt d'une définition fonctionnelle de la signature électronique n'est-il pas justement de préciser les différentes fonctions assignées à celle-ci ?

Plus fondamentalement, on peut se demander si l'imputation de la signature à une personne déterminée implique nécessairement l'imputation à cette dernière du contenu de l'acte signé ? Par ailleurs, l'imputabilité d'un contenu implique-t-il de soi la volonté d'y adhérer ? Qu'en est-il, en d'autres termes, de l'*animus signandi* ?

Notre première interrogation précédemment énoncée est d'autant plus aiguë que n'apparaît pas explicitement, dans l'article 1322, alinéa 2, la nécessité d'un lien, sinon physique, au moins logique, entre l'acte et la signature. On observe, en effet, que, s'écartant du texte de la directive (« *une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques* (...) » (69)), le législateur belge se contente d'« *un ensemble de données électroniques pouvant être imputé à une personne déterminée* (...) ». Cela étant, lorsqu'il est question d'une signature numérique fondée sur la cryptographie asymétrique, la signature est le résultat d'une transformation de l'écrit par application d'une clé de chiffrement. En pareil cas, on conçoit assez aisément que l'imputation d'un ensemble de données électroniques à une personne déterminée puisse impliquer son adhésion au contenu de l'acte. Mais, cette déduction repose, de toute évidence, sur un présupposé technique, qui n'a pas vraiment sa place dans une définition fonctionnelle de la signature. En tout état de cause, il n'est guère possible d'accorder une valeur juridique à une signature électronique si elle n'est pas jointe ou liée logiquement au contenu sur lequel l'auteur marque son consentement.

Par ailleurs – à propos de la seconde interrogation –, il ressort de la jurisprudence (notamment celle relative à la place de la signature (70)) que la présence d'une signature que l'on peut rattacher à une personne déterminée ne dispense pas le juge de rechercher si cette dernière a effectivement voulu marquer son adhésion au contenu de l'acte. On ne saurait donc estimer que l'imputabilité de la signature implique *en tout état de cause* l'adhésion au contenu. En revanche, la signature *reconnue ou non contestée* crée une présomption *juris et de jure* que le signataire a donné son consentement au contenu de l'acte (71). En pratique, on

---

(63) JOUE 15 juill. 2003, n° L 175/45. **(64)** En doctrine belge, voir en particulier, outre les traités relatifs au droit de la preuve, l'étude classique de M. Van Quickenborne, Quelques réflexions sur la signature des actes sous seing privé, note sous Cass., 28 juin 1982, R.C.J.B., 1985, p. 57 et s. **(65)** Carbonnier J., Droit civil. 1/ Les personnes, Thémis, Paris, P.U.F., 1996, p. 50, n° 27. **(66)** S'il prétend échapper aux conséquences de sa signature, il devra établir l'existence d'un vice de consentement ou une simulation. Voir Van Quickenborne M., précité, spéc. p. 69-70, n^{os} 5 et 6. **(67)** Du reste, l'on n'a pas connaissance de litiges qui se soient véritablement noués à propos de la signature en ces hypothèses très particulières. **(68)** Justification de l'amendement n° 12 (du Gouvernement) à la Proposition de loi introduisant de nouveaux moyens de télécommunication dans la procédure judiciaire et extrajudiciaire (13 juin 2000), Doc. parl., Ch. repr., sess. ord. 1999-2000, doc 50 0038/006, p. 11, et le rapport fait au nom de la Commission de la justice par Bart Somers (30 juin 2000), Doc. parl., Ch. repr., sess. ord. 1999-2000, doc 50 0038/008, p. 30. **(69)** Art. 2, 1. À ce propos, voir les observations formulées par le Service juridique de la Chambre au sujet de l'amendement n° 12, Doc. parl., Ch. repr., sess. 1999-2000, doc 50 0038/008, p. 32. **(70)** Voir Verheyden-Jeanmart N., précité, p. 240-242, n^{os} 508 et s., et les références.

considérera que l'*animus signandi* se manifeste, par exemple, lors de la saisie, par le signataire, du code secret permettant l'activation de sa clé cryptographique. Néanmoins, il n'est pas exclu qu'un juge estime, en cas de contestation, que telle signature électronique, bien qu'imputable à telle personne, n'atteste pas son intention de s'approprier le contenu de l'acte. Même si cette condition n'est pas inscrite explicitement dans le texte, elle y figure implicitement sous la notion d'imputabilité éclairée par les travaux préparatoires, et se déduit, du reste, de la théorie générale de la signature.

Curieusement, la fonction d'adhésion au contenu de l'acte est, comme telle, absente dans la directive du 13 décembre 1999, alors qu'elle apparaissait clairement dans la première version de la proposition de directive (72). Faut-il estimer que, dans l'esprit du législateur européen, la fonction de validation du consentement au contenu d'un acte n'est pas une condition de la signature électronique ? Manifestement oui, la « *signature* » y apparaît comme un procédé technique visant à garantir l'origine de données et le maintien de leur intégrité.

Quelle position le droit belge adopte-t-il eu égard à cette question ?

Selon la définition de l'article 2, 1°, de la loi du 9 juillet 2001, on entend par signature électronique « *une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification* ».

Initialement, le parti avait été pris de ne pas intégrer cette définition (73), mais il en a été décidé autrement suite à un amendement du Gouvernement (74). Cet ajout est justifié par le fait que les annexes du texte de loi font référence au terme défini et par un souci de simplicité, de lisibilité et de plus grande cohérence par rapport à la directive (75).

Au contraire de la définition de la signature électronique figurant dans le Code civil (art. 1322, al. 2) qui conçoit l'identification d'une personne dans ses rapports avec un acte dont elle s'approprie le contenu, la définition de l'article 2, 1, de la directive – reprise à l'article 2, 1°, de la loi du 9 juillet 2001 – désigne toute méthode d'*authentification*. Or, cette dernière notion d'une part, ne conduit pas nécessairement à l'identification d'une personne, d'autre part, peut s'avérer sans rapport avec l'approbation du contenu d'un acte juridique. Il peut s'agir d'un simple procédé destiné à reconnaître un « *objet* ». Ainsi, l'authentification peut porter sur l'origine et l'intégrité de données, voire sur d'autres éléments tels qu'un serveur web, un routeur, une œuvre numérique protégée ou un logiciel (76)... Cette approche technique de la signature – censée se rapporter non seulement à des actes juridiques, mais aussi à d'autres objets – s'accorde mal avec notre tradition juridique selon laquelle seule une personne peut signer un acte afin de s'identifier et de marquer son adhésion au contenu de ce dernier.

La définition de la « *signature électronique avancée* », également introduite en notre droit, n'intègre pas davantage la fonction d'adhésion au contenu de l'acte.

La réception en droit belge de ces définitions de la signature électronique conduira-t-elle la doctrine et la jurisprudence belge à faire droit à la signature électronique en sa seule fonction d'« *authentification* », indépendamment de tout lien avec un acte juridique ? Admettra-t-on une forme de signature technique (comme cela semble être le cas en matière de facturation électronique), aux côtés de la signature telle qu'elle est traditionnellement comprise en droit ? Sans doute est-il trop tôt pour se prononcer sur ces questions. Quoi qu'il en soit, il est certain qu'à ce jour, on ne relève aucun signe de la moindre volonté de s'écarter de notre conception traditionnelle de la signature au sens juridique de la notion.

(...) il sera difficile de convaincre un juge de la valeur probatoire des documents électroniques produits sans une bonne documentation du processus de numérisation, de conservation et de datation électronique de ceux-ci.

B. – Régime de la preuve de la signature électronique et archivage

Le régime de la preuve de la signature électronique peut-il ne pas inclure des dispositions relatives à l'archivage ? N'est-il pas nécessaire de documenter soigneusement le processus de dématérialisation par une politique d'archivage ?

Qu'il nous soit permis de répondre brièvement à ces questions encore peu traitées. Actuellement, les clés de la première génération n'ont pas encore été craquées de sorte qu'un archivage « normal » paraît suffire. Par contre, dès l'instant où les clés auront été craquées, un archivage rigoureux s'avèrera sans doute nécessaire afin que le juge reconnaisse que les documents signés à l'époque par des clés de première génération n'ont pas été manipulés depuis.

Une autre question concerne la datation des opérations. À l'heure actuelle, le recours à l'horodatage est peu fréquent. On se contente généralement de se baser sur l'heure indiquée par l'horloge de l'ordinateur. La fiabilité de la méthode est naturellement sujette à caution comme en attestent quelques décisions de jurisprudence (77).

Pratiquement, on se doute qu'il sera difficile de convaincre un juge de la valeur probatoire des documents électroniques produits sans une bonne documentation du processus de numérisation, de conservation et de datation électronique de ceux-ci. Encore subsiste-t-il de nombreuses inconnues sur la valeur juridique des processus et documents dématérialisés.

L'attention du législateur a été attirée sur la nécessité de se doter d'un cadre juridique pour les « *services de confiance* » tels l'archivage de documents électroniques, l'horodatage et le recommandé électronique. Les acteurs du marché réclament avec force des règles et garanties claires en la matière. L'Observatoire des Droits de l'Internet a plaidé en ce sens dans son avis n° 3 (78).

>

(71) Van Quickenborne M., précité, spéc. p. 69-70, n^{os} 5 et 6. Les travaux préparatoires de la loi du 20 octobre 2000 confirment explicitement ce point de vue général. Voir Justification de l'amendement n° 12 (du Gouvernement) à la Proposition de loi introduisant de nouveaux moyens de télécommunication dans la procédure judiciaire et extrajudiciaire (13 juin 2000), Doc. parl., Ch. repr., sess. 1999-2000, doc 50 0038/006, p. 11, et le rapport fait au nom de la Commission de la justice par Bart Somers (30 juin 2000), Doc. parl., Ch. repr., sess. 1999-2000, doc. 50 0038/008, p. 30. **(72)** Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, JOCE 23 oct. 1998, n° C 325, p. 1 : « *Aux fins de la présente directive, on entend par signature électronique une signature sous forme numérique intégrée, jointe ou liée logiquement à des données, utilisée par un signataire pour signifier son acceptation du contenu des données* (...) ». **(73)** Exposé des motifs du projet de loi relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques, Doc. parl., Ch. repr., sess. ord. 1999-2000, n° 0322/001, p. 18-19. Cette définition est estimée difficilement compatible avec notre conception traditionnelle de la signature. **(74)** Amendement n° 1 du Gouvernement (10 nov. 2000), Doc. parl., Ch. repr., sess. ord. 1999-2000, n° 0322/002, p. 1. **(75)** Précité, p. 18-19. **(76)** À ce sujet, voir Caprioli E., La loi française sur la preuve et la signature électroniques dans la perspective européenne (Dir. 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999), JCP G, doctr. I 224, p. 787 et s., spéc. p. 790, n° 10 ; Antoine M. et Gobert D., La directive européenne sur la signature électronique : vers la sécurisation des transactions sur l'internet ?, J.T.D.E., 2000, n° 68, p. 74 ; Gobert D. et Montero É., L'ouverture de la preuve littérale aux écrits sous forme électronique, J.T., 2001, p. 116. **(77)** Pour une illustration, voir Gand (7^{e} ch.), 10 mars 2008, Computerr., 2008, p. 301, note Van Eecke P. et Verbrugge E., D.A.O.R., note Montero É. (à paraître). **(78)** Avis n° 3 relatif aux pistes pour renforcer la confiance dans le commerce électronique (1er juin 2004), <www.internet-observatory.be/internet_observatory/pdf/advices/advice_fr_003.pdf>.

L'absence de cadre juridique représente de toute évidence un frein au développement de ces services. Ainsi, dans la mesure où les coûts liés à l'archivage électronique ne sont pas négligeables, les entreprises souhaitent des indications *précises* sur les méthodes qui sont reconnues par le législateur. Les acteurs du marché (tant les prestataires d'archivage électronique que les entreprises qui envisagent de recourir à leurs services) ont ainsi exprimé le souhait que le législateur clarifie les points suivants : *stipuler la validité du recours à l'archivage électronique*, à certaines conditions, lorsque la loi exige, de manière expresse ou tacite, la conservation d'un document ; permettre aux entreprises qui le souhaitent d'*archiver elles-mêmes leurs documents en interne*, sans recourir aux services d'un tiers (79) ; *permettre la numérisation des documents papier*, puis la destruction des originaux, tout *en accordant une valeur juridique aux copies numérisées* ; enfin, *définir les critères de qualité auxquels doivent répondre les prestataires de services d'archivage électronique* pour être reconnus comme fiables.

Il s'agit non seulement de fixer les obligations et responsabilités à charge des prestataires de services de confiance mais aussi de prévoir un certain nombre de présomptions ou d'assimilations en faveur des documents issus de services ou de systèmes conformes aux exigences inscrites dans la loi. Un premier pas a été fait dans cette direction avec l'adoption d'une loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance (80). Mais, il s'agit d'un texte encore très timide dès lors que l'essentiel du dispositif devait figurer dans les arrêtés royaux d'exécution qui, malheureusement n'ont pas été adoptés dans le délai d'habilitation accordé au Roi. Pratiquement, tout reste donc à (re)faire en la matière. D'ailleurs, un nouveau texte de loi, plus ambitieux, est actuellement en préparation. ◆

---

(79) Il serait discriminatoire de ne reconnaître une valeur légale qu'aux documents archivés par un tiers conformément à certaines règles de l'art, et de nier toute valeur légale aux mêmes documents, archivés selon les mêmes règles, mais en interne, par l'entreprise concernée. **(80)** M.B., 17 juill.2007, p. 38587.