La directive européenne sur la signature électronique : vers la sécurisation des transactions sur l'Internet?

Gobert, Didier; Antoine, Mireille

Published in:
Journal des Tribunaux. Droit Européen

Publication date:
2000

Document Version
le PDF de l'éditeur

Mireille ANTOINE et Didier GOBERT, *JTDE*, avril 2000, n° 68, pp. 73 à 78.

"LA DIRECTIVE EUROPEENNE SUR LA SIGNATURE ELECTRONIQUE. VERS LA SECURISATION DES TRANSACTIONS SUR L'INTERNET ?"

Mireille ANTOINE
Chercheur au Centre de Recherches Informatique et Droit
FUNDP - Namur

Didier GOBERT
Assistant à la faculté de droit de Namur
Chercheur au Centre de Recherches Informatique et Droit
Consultant en droit de l'informatique (www.consultandtraining.com)

Publié dans *JTDE*, avril 2000, n° 68, pp. 73 à 78.

I.- INTRODUCTION

1. L'essor des communications en réseau ouvert et plus particulièrement du commerce électronique nécessite non seulement le développement de nouvelles techniques de signature, mais également leur reconnaissance juridique. A cette fin, la Commission européenne a présenté le 16 juin 1998 une proposition de directive sur un cadre commun pour les signatures électroniques[1]. Suite aux quelques discussions animées, une nouvelle version a été présentée au Conseil des ministres européen du 22 avril 1999 et a fait l'objet d'une position commune[2]. Le texte étant soumis à la procédure de codécision, il a été présenté au Parlement européen pour d'éventuels amendements, et a enfin été adopté le 13 décembre 1999[3].

Cette directive résulte du constat que des initiatives législatives se multiplient dans plusieurs Etats membres et qu'il devient dès lors urgent de disposer d'un cadre juridique harmonisé au niveau européen. Ce dernier est justifié pour, d'une part, éviter que le fonctionnement du marché intérieur ne soit gravement entravé par des initiatives divergentes, d'autre part, encourager l'utilisation des signatures électroniques et, enfin, renforcer la confiance dans les nouvelles technologies et favoriser ainsi leur acceptation générale. A ces fins, la directive poursuit essentiellement deux objectifs majeurs. Le premier est la reconnaissance juridique

1 Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, COM (98)297 final, 13 juin 1998, *J.O.C.E.*, C 325/5-11 du 23 octobre 1998 ou http://www.ispo.cec.be/eif/policy/com98297fr.doc. Pour un commentaire approfondi de la première version de cette proposition de directive, voy. R. JULIA-BARCELO et T.C. VINJE, "Electronic signatures - another step towards a European framework for electronic signatures : the Commission's Directive proposal", *Computer Law & Security Report*, octobre 1998, n° 14/5, pp. 303-313.

2 Voy. l'URL suivant : http://europa.eu.int/comm/dg15/fr/media/sign/index.htm

3 Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, L 13 du 19 janvier 2000, pp. 12 à 20.

des signatures électroniques (1). Le second est la création d'un cadre légal pour l'activité des prestataires de service de certification (ci-après PSC) (2).

II.- RECONNAISSANCE LÉGALE DES SIGNATURES ÉLECTRONIQUES

2. Le premier objectif poursuivi par la directive est la reconnaissance légale des signatures électroniques. Celles-ci ne pourront en effet favoriser le commerce électronique que si une valeur juridique leur est reconnue. Or dans la plupart des Etats membres, les exigences légales relatives à la preuve, et plus particulièrement à la signature, ne sont estimées satisfaites que pour la signature manuscrite.

Afin d'atteindre l'objectif visé ci-dessus, la directive entend tout d'abord définir la signature électronique (A) pour ensuite réglementer ses effets juridiques (B). On s'interrogera enfin sur la reconnaissance de la signature des personnes morales (C).

3. L'analyse de la démarche adoptée par la directive appelle deux observations préalables. Premièrement, celle-ci ne couvre pas les aspects relatifs à la validité des contrats. Dès lors, il n'est pas demandé aux Etats membres de supprimer les exigences formelles relatives à la conclusion des contrats, mais plutôt de reconnaître que, lorsqu'un écrit signé est exigé, ces exigences peuvent être remplies par la signature électronique. Deuxièmement, elle ne s'applique pas aux signatures utilisées en réseau fermé[4]. La Commission considère à ce propos que le principe de la liberté contractuelle doit prévaloir.

A.- Le concept de signature électronique

4. La directive donne une double définition de la signature électronique. D'une part, elle définit de manière très générale le terme *signature électronique* comme *« une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification »* (article 2, 1.). D'autre part, elle propose une définition d'une catégorie particulière de signature électronique qu'elle qualifie de *signature électronique avancée* (article 2, 2.) :

4 Encore faut-il s'entendre sur la notion de réseau fermé, non définie par la directive.

On entend par signature électronique avancée, une signature électronique qui satisfait aux exigences suivantes :

a) être liée uniquement au signataire ;

b) permettre d'identifier le signataire ;

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

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

L'objet de cette distinction n'est pas claire. Elle a manifestement été inspirée par les travaux de la CNUDCI[5]. La directive a probablement voulu attirer l'attention sur le fait qu'il existe une multitude de techniques baptisées « signature électronique », dès lors qu'elles permettent, à elles seules ou en combinaison, de réaliser les fonctions dévolues à la signature[6]. Cependant, toutes ne présentent pas nécessairement un niveau de sécurité acceptable sur le plan juridique. Le point 1 des définitions vise certainement à englober ces différents mécanismes, sans toutefois leur reconnaître une valeur juridique comparable à celle de l'écrit papier signé manuscritement (voir ci-après). On suppose que c'est à dessein que la définition parle de « donnée servant de méthode d'authentification », l'authentification pouvant porter tant sur l'origine des données que sur leur intégrité, voire sur d'autres éléments. Par cette définition, la directive a voulu affirmer sa neutralité technologique en ne privilégiant aucun mécanisme particulier de signature électronique.

Cette neutralité technologique est toutefois tempérée par le point 2) dans lequel on considère que certaines signatures électroniques peuvent être avancées, et donc sécurisées, pour autant qu'elles satisfassent aux exigences de cet article. Ces exigences, présentées de manière technique, consacrent en réalité les fonctions d'identification (point b[7]) et d'intégrité (point d).

---

5 Voir, par exemple, Commission des Nations Unies pour le Droit Commercial International, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente-troisième session (New York, 29 juin-10 juillet 1998), A/CN.9/454, 21août 1998. Voir aussi http://www.un.or.at/uncitral/fr-index.htm.

6 Pour une analyse approfondie des fonctions de la signature, voir D. Gobert et E. Montero, "La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle", Cahiers du C.R.I.D., n° 17, Bruxelles, Bruylant, 2000, *à paraître*.

7 Les points a) et c) ne font que stipuler les conditions préalables à l'exigence d'identification du signataire : en effet, une donnée ne permettrait pas d'identifier le signataire, et d'éviter les risques de répudiation, si cette même donnée était liée à plusieurs signataires ou si elle était créée et gérée par plusieurs personnes.

La neutralité technologique de cette définition n'est qu'apparente dans la mesure où il ne fait pas de doute qu'actuellement, seule la technique de la signature digitale[8], fondée sur la cryptographie asymétrique, répond à la définition de la signature électronique avancée. Le contenu des annexes ne laisse planer aucune incertitude à ce sujet.

B.- Les effets juridiques de la signature électronique : changement ou *statut quo* ?

5. L'intérêt de la distinction évoquée ci-dessus se fait ressentir dans l'article 5, qui traite des effets juridiques de la signature électronique. Afin de reconnaître une valeur juridique à cette dernière, l'article 5 contient deux clauses : l'une d'assimilation (article 5.1.) et l'autre de non discrimination (article 5.2.).

1. *Les Etats membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature :*
   a) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier, et
   b) soient recevables comme preuve en justice.

2. *Les Etats membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique 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 de service de certification accrédité, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature.*

---

8 Pour une explication détaillée de cette technique, appelée aussi *signature numérique*, voir S. PARISIEN et P. TRUDEL, *L'identification et la certification dans le commerce électronique*, Québec, Ed. Yvon Blais Inc., 1996, pp. 93 à 113; J. HUBIN, *La sécurité informatique, entre technique et droit*, Cahiers du C.R.I.D., n° 14, E. Story-Scientia, 1998, spéc. pp. 68-112 ; M. Antoine et D. Gobert, "Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification", *R.G.D.C.*, juillet-octobre 1998, n° 4/5, pp. 292 à 295.

6. La clause d'assimilation (article 5.1.) consiste à assimiler la signature électronique à la signature manuscrite lorsque certaines conditions sont remplies[9], c'est-à-dire à considérer que la signature électronique doit être recevable comme preuve en justice et qu'elle doit bénéficier de la force probante[10] accordée à la signature manuscrite. Notons que cette clause d'assimilation ne profite pas à l'ensemble des mécanismes de signature électronique, mais uniquement aux signatures électroniques avancées (pour autant que les conditions de l'article 2.2. soient remplies).

D'un point de vue légistique, il est étonnant que l'article 5.1. commence par traiter de la force probante (point a) des signatures électroniques avancées pour ensuite envisager leur recevabilité (point b), puisque celle-ci est un préalable et une condition indispensable de leur reconnaissance juridique.

7. La clause de non discrimination (article 5.2.) s'applique lorsque les conditions auxquelles est subordonnée l'application de la clause d'assimilation ne sont pas remplies. Dans ce cas, les Etats membres doivent veiller à ce que l'efficacité juridique[11] et la recevabilité comme preuve en justice d'une signature électronique ne soient pas refusées pour le seul motif que la signature se présente sous forme électronique, ou qu'elle ne repose pas sur un certificat qualifié, ou encore qu'elle ne repose pas sur un certificat délivré par un PSC accrédité au sens de la directive. Le principe énoncé dans cet article doit être entendu comme celui de la recevabilité[12] des signatures électroniques *lato sensu*, ce qui constitue en soi un énorme progrès par rapport aux règles traditionnelles du droit de la preuve. Toutefois, à défaut de répondre aux spécifications de l'article 5.1., il appartient à celui qui s'en prévaut de convaincre le juge de sa valeur probante[13].

---

9 La signature électronique doit être avancée au sens de l'article 2, 2., elle doit reposer sur un certificat qualifié tel que défini à l'article 2, 10, et enfin elle doit être créée par un dispositif sécurisé de création de signature tel que décrit à l'annexe 3 de la directive.

10 Par force probante, en entend « l'intensité quant à la preuve que la loi lui reconnaît et qui s'impose au juge ». F. DUMON, « De la motivation des jugements et arrêts et de la foi due aux actes », *J.T.*, 1978, p. 486.

11 On peut s'interroger sur la signification concrète de ce concept « d'efficacité juridique » !

12 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 ». Cela ne signifie donc pas que l'élément dit recevable aura forcément une influence sur la décision du juge ; celui-ci peut parfaitement considérer que ledit élément ne prouve rien. Il n'a qu'une seule obligation : étudier l'élément en question.

13 Sur les conséquences de la distinction recevabilité/valeur probante, D. Gobert et E. Montero, *op.cit.*

8. La formulation de l'article 5 appelle deux commentaires.

Puisque l'article 5.1. traite de la force probante des signatures électroniques avancées, il n'était pas nécessaire de traiter dans un second temps de leur recevabilité étant donné que celle-ci est une condition *sine qua non* de leur reconnaissance juridique. Il eut donc été plus clair de poser, dans un premier temps, le principe de la recevabilité de toute signature électronique et de traiter, dans un second temps, de la force probante des signatures électroniques avancées. De plus, cela aurait évité de devoir traiter du problème de la recevabilité dans la clause d'assimilation (art. 5, 1, b), comme évoqué plus haut.

Ensuite, on peut observer qu'en pratique, l'article 5.1. de la directive ne présente un intérêt que si les Etats membres, tout en respectant le principe de la liberté d'exercice de l'activité de certification, mettent sur pied un régime d'accréditation des PSC[14]. En dehors de toute initiative nationale en vue de l'accréditation de ceux-ci, la personne qui se prévaut d'un document signé électroniquement serait tenue d'apporter la preuve que les conditions fixées par les trois annexes de la directive ont effectivement été remplies afin de bénéficier de la clause d'assimilation. Cette situation est difficilement acceptable, surtout si la charge de la preuve incombe au consommateur, étant donné la difficulté d'apporter une telle preuve[15]. Or, elle semble envisageable en pratique.

On peut dès lors craindre que l'objectif visé par la directive, à savoir renforcer la sécurité juridique, soit manqué puisque, quand bien même le texte résoudrait-il la question de la recevabilité des documents signés électroniquement, le pouvoir discrétionnaire du juge quant à l'appréciation de leur valeur probante serait de nature à rendre l'issue du litige incertaine.

En poussant le raisonnement plus loin, on constate que la combinaison des effets de la clause d'assimilation en droit belge et de la notion de certificat qualifié peut avoir des conséquences désastreuses. En effet, pour rappel l'article 5.1. stipule que si certaines conditions sont

---

14 L'octroi d'une accréditation est nécessairement subordonné au respect des conditions prévues à l'annexe II, ce qui suppose la mise en place d'une procédure de délivrance de l'accréditation et un contrôle préalable (sous la forme d'un audit) du respect de ces conditions.

15 Cette critique doit néanmoins être tempérée par le point a) de l'annexe II qui stipule que « Le prestataire de service de certification qui délivre des certificats qualifiés doit faire la preuve qu'il est suffisamment fiable pour fournir des services de certification ». Dans ce cadre, on peut imaginer que la personne qui se prévaut de la signature mette le prestataire à la cause afin qu'il collabore pour apporter, voire qu'il apporte lui-même, cette preuve difficile.

remplies, la signature électronique avancée doit bénéficier des mêmes effets juridiques que ceux qui sont reconnus à la signature manuscrite. En droit belge, cet effet n'est autre que la force probante. Cela signifie qu'un écrit signé manuscritement s'impose au juge (on parle de preuve *parfaite*)[16]. Or, l'une des conditions implique que la signature électronique soit basée sur un certificat qualifié. La notion de certificat qualifié est définie dans l'article 2 comme *un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II.* Cette définition ne semble pas exiger qu'un prestataire s'engage dans une procédure d'accréditation pour que les certificats qu'il délivre soient réputés «qualifiés ». Le prestataire pourrait donc se limiter à prétendre qu'il satisfait aux conditions d'accréditation (voir à ce propos l'annexe II de la directive) sans toutefois demander cette dernière et sans que le respect effectif de ces conditions ne fasse l'objet d'aucun contrôle.

Il est logique qu'on reconnaisse force probante aux signatures électroniques avancées liées à un certificat émis par un PSC accrédité car ce dernier est soumis au contrôle permanent d'un tiers indépendant. Ainsi, on considère qu'il opère dans des conditions de fiabilité et de sécurité optimales. Par contre, il paraît plus douteux de reconnaître cette même force probante en l'absence d'accréditation[17]. En effet, il en résulte que la prétention selon laquelle le PSC répond aux exigences de l'annexe II ne fait l'objet d'un contrôle, ni *a priori* dans le cadre d'une accréditation ni *a posteriori* par le juge dans le cadre d'un litige[18]. Dans cette optique, on peut également s'interroger sur l'intérêt pour un prestataire de s'engager dans une procédure d'accréditation.

On peut une nouvelle fois craindre que l'objectif de renforcer la sécurité juridique, poursuivi par la directive, soit mis en péril.

---

16 En d'autres mots, lorsqu'un écrit signé manuscritement est présenté au juge, cet élément de preuve doit non seulement être déclaré recevable par le juge, mais en plus il doit être considéré comme représentant une manifestation fiable de la réalité, sans qu'il ne dispose du pouvoir d'apprécier sa valeur.

17 Pourtant, cela découle de la combinaison des articles 2, 10) et 5.1.

18 Sauf pour une partie à contester la signature et donc éventuellement le respect des exigences de l'annexe II, preuve diabolique…

C.- La signature des personnes morales : une avancée significative ?

9. La directive définit dans son article 2, 3° le « signataire » comme *toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une entité ou personne physique ou morale qu'elle représente.* Cette définition peut être interprétée très largement. En effet, on parle de « toute personne » sans aucune distinction, ce qui laisse supposer que cela vise tant les personnes physiques que morales. Cette vision du concept de signataire était déjà préconisée par la Commission européenne qui, dans sa communication du 8 octobre 1997[19], indiquait dans le point 2.3., (i) que « Les clés (et par conséquent les certificats) peuvent être allouées à des personnes privées ou juridiques (par exemple une société à responsabilité limitée)… ». La directive ne semble donc pas exclure la signature des personnes morales, déjà reconnue au Royaume-Uni.

La Belgique (ainsi que le Luxembourg) vient de déposer un projet de loi allant dans ce sens puisqu'il reconnaît expressément, dans son article 4, §4, la signature des personnes morales[20]. Cela signifie qu'un document électronique, dont la signature électronique avancée est combinée à un certificat qualifié émis au nom d'une personne morale[21], doit être considéré comme un acte sous seing privé et permettre de faire preuve au même titre qu'un écrit signé par une personne physique. De plus, cela implique que les personnes morales peuvent valablement conclure des contrats via les messages électroniques signés par elles.

Du point de vue des conséquences juridiques, il paraît logique de reconnaître la signature des personnes morales. Si elle n'existe pas matériellement, la personne morale existe juridiquement et, à ce titre, elle est apte à être titulaire de droits et obligations et est susceptible de voir son patrimoine engagé. Dès lors, on peut admettre qu'une personne morale, qui peut être identifiée et engagée juridiquement, puisse signer car la signature n'a d'autre but que de prouver la volonté du signataire d'être engagé.

---

19 COM(97)503 : « Vers un cadre européen pour les signatures numériques et le chiffrement : assurer la sécurité et la confiance dans la communication électronique », Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions, 8 octobre 1997.

20 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., 16 décembre 1999, n° 322.

21 C'est-à-dire sans référence aucune à la personne physique qui met en œuvre la signature.

Il est vrai que jusqu'à présent, cette question ne s'était pas réellement posée dans le contexte papier, car la signature ne pouvait être que manuscrite. En pratique, une personne morale, qui n'a pas d'existence matérielle, pouvait difficilement signer manuscritement. Dans le monde électronique, par essence immatériel, il en va différemment. En effet, la signature ne se réduit plus à une marque apposée de manière manuscrite, mais peut désormais être réalisée au moyen d'une technique informatique qui peut être mise en œuvre aussi bien par une personne physique que par une personne morale et qui permet d'identifier cette dernière.

La position adoptée par l'Union se situe dans la lignée de mouvements amorcés dans certains Etats membres, comme la Belgique[22] et la France, allant dans le sens d'une « responsabilisation plus poussée des personnes morales », en reconnaissant la responsabilité pénale des personnes morales.

III.- CRÉATION D'UN CADRE LÉGAL POUR LE FONCTIONNEMENT DES PRESTATAIRES DE SERVICE DE CERTIFICATION

10. Après avoir fixé les principes généraux concernant l'accès au marché (A), la directive entend mettre sur pied un mécanisme de certification fiable. Ce mécanisme s'articule autour de trois points essentiels : tout d'abord celui de la responsabilité des PSC (B), ensuite celui de la protection des données personnelles (C), enfin celui de la reconnaissance, sous certaines conditions, de certificats délivrés par des PSC établis dans des pays tiers (D).

A.- Principes introductifs

11. Les nouvelles techniques de signature permettent au destinataire de données signées électroniquement de vérifier l'identité du signataire et l'intégrité des données reçues. Toutefois, la confiance dans un mécanisme de signature électronique, et spécialement dans un mécanisme de signature basé sur la technique de cryptographie asymétrique, dépend de

[22] Loi du 4 mai 1999 instaurant la responsabilité pénale des personnes morales, *M.B.*, 22 juin 1999.

l'intervention de tierces parties qui pourront certifier le lien entre une personne et son dispositif de création de signature par l'émission de certificats[23].

12. Le principe posé par la directive est celui de la liberté de fourniture des services de certification. Les Etats membres ne peuvent soumettre celle-ci à aucune autorisation préalable. De même, ils ne peuvent limiter le nombre de PSC. Toutefois, deux tempéraments viennent considérablement modérer le principe formulé.

D'une part, les Etats membres **peuvent**, tout en respectant le principe de la liberté d'exercice de l'activité de certification, instaurer ou maintenir des régimes volontaires d'accréditation visant à améliorer le niveau de service fourni (article 3.2.). Les critères d'accréditation doivent dans ce cas être « objectifs, transparents, proportionnés et non discriminatoires ». En Belgique, par exemple, le respect de ces critères semble faire défaut dans le cadre du système d'accréditation mis en place par la Banque Carrefour de Sécurité Sociale. En effet, l'Arrêté Royal du 16 octobre 1998[24] ne souffle mot ni de la procédure ni des conditions relatives à l'accréditation.

D'autre part, les Etats membres **doivent** veiller à contrôler les PSC établis sur leur territoire délivrant des certificats qualifiés (article 3.3). En réalité, la directive ne revêt d'intérêt que si les Etats membres, tout en respectant le principe de la liberté d'activité de certification, instaurent un régime volontaire d'accréditation.

B.- Responsabilité des prestataires de service de certification

13. Les dispositions relatives à la responsabilité des PSC sont particulièrement importantes car elles conditionnent la confiance que les utilisateurs pourront placer dans un régime de certification.

---

23 Il convient de souligner qu'outre la délivrance et la gestion de certificats, les prestataires de service de certification peuvent être amenés à offrir d'autres services et produits tels que les services d'enregistrement, les services horodateurs, les services d'annuaires, …

24 Arrêté Royal du 16 octobre 1998 « portant des dispositions relatives à la signature électronique, qui s'applique à la sécurité sociale, en application de l'article 38 de la loi du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions », *M.B.*, 7 novembre 1998, prolongé par l'Arrêté Royal du 11 avril 1999, *M.B.*, 2 juillet 1999.

L'article 6 de la directive relatif à la responsabilité doit être lu à la lumière de son annexe II fixant les *exigences concernant les prestataires de service de certification délivrant des certificats qualifiés*. De l'analyse conjointe de ces textes, il ressort que les obligations incombant aux PSC peuvent être classées en deux catégories. La première est relative à l'objet de leur l'activité. La seconde a trait au fonctionnement du mécanisme de certification. Avant toute chose, il convient de délimiter le champ d'application des dispositions relatives à la responsabilité.

1.- Champ d'application

14. La directive ne traite des questions relatives à la responsabilité qu'à propos des certificats émis par les PSC qui délivrent au public des certificats présentés comme qualifiés ou qui garantissent publiquement de tels certificats. Dès lors, pour les PSC qui délivrent des certificats ordinaires (qui ne sont pas présentés comme qualifiés), les différentes législations nationales relatives à la responsabilité de droit commun trouvent à s'appliquer. La différence de régime de responsabilité est justifiée par le fait que des conséquences juridiques propres sont attachées aux certificats qualifiés.

Pour les certificats qualifiés, la directive établit un régime spécifique de responsabilité. Celui-ci tente d'établir un équilibre entre les intérêts des PSC et ceux des utilisateurs de certificats, c'est-à-dire « toute personne qui se fie légitimement au certificat ». La directive ne traite donc pas des questions relatives à la responsabilité qui pourraient se poser dans le cadre des relations entre les PSC et les titulaires de certificats, ni aux relations éventuelles entre PSC et autorités d'enregistrement. Ici aussi, à défaut de règles spécifiques, les différentes législations nationales sont d'application.

2.- L'exactitude comme essence de la certification

15. Les obligations énumérées à l'article 6 visent toutes à assurer l'exactitude des informations mises à la disposition des utilisateurs. L'exactitude constitue l'essence même de la fonction de certification : elle conditionne la confiance que les utilisateurs peuvent placer dans un mécanisme de certification. Les obligations mises à charge des PSC portent sur les trois points suivants : l'exactitude des informations contenues dans le certificat, la vérification

de la détention et de la complémentarité des données afférentes à la création de signature et, enfin, la révocation des certificats.

16. ***Exactitude des informations contenues dans le certificat*** - Les PSC qui délivrent au public des certificats présentés comme qualifiés, ou qui garantissent publiquement de tels certificats, doivent garantir l'exactitude des informations contenues dans le certificat qualifié à la date de sa délivrance (article 6,1.a). Puisqu'une obligation d'exactitude pèse sur le prestataire à ce moment précis, il doit veiller à ce que la date et l'heure d'émission du certificat puissent être déterminées avec précision (annexe II, b).

Si la directive prévoit une obligation d'exactitude des informations contenues dans le certificat au moment précis de son émission, et non à dater de ce moment, c'est parce qu'il ne peut raisonnablement lui être demandé d'assurer un contrôle permanent des informations contenues dans le certificat. Un devoir de vigilance pèse donc sur le titulaire du certificat qui se voit, indirectement, reconnu titulaire de diverses obligations. Il doit non seulement tout mettre en œuvre afin que soit préservée la confidentialité de son dispositif de création de signature, mais il doit également communiquer au PSC ayant émis le certificat toute modification relative aux données du certificat et, en cas de doute quant au maintien de la confidentialité des données afférentes à la création de signature, faire procéder à la révocation du certificat.

17. ***Détention et complémentarité des données afférentes à la création et à la vérification de signature*** - Le PSC doit garantir que le signataire identifié dans le certificat détient effectivement *les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat* (article 6,1.b). Par souci de simplification, et pour illustrer notre propos, nous parlerons plutôt de clé publique et de clé privée, sachant qu'elles sont respectivement une application des données afférentes à la vérification de signature et à la création de signature.

L'obligation de vérification dont question ci-dessus pèse sur tout PSC, qu'il soit ou non chargé de générer les clés publiques et privées. L'obligation de vérification de la détention des clés sous-tend-elle l'obligation de vérification de leur complémentarité ? Si la directive impose explicitement cette obligation de vérification de la complémentarité des clés aux PSC

qui les génèrent (article 6, 1, c), il semble qu'elle ne fasse pas peser cette obligation sur les prestataires qui ne les génèrent pas.

Or, cette obligation est fondamentale et devrait, selon nous, peser sur tout PSC qui offre au public le niveau de certification voulu par la directive. En effet, en émettant un certificat, le prestataire confirme le lien entre une personne et sa clé publique. La certification demeure vide de sens si, certifiant ce lien, le PSC omet de vérifier la complémentarité des clés. Le dispositif de vérification n'est, comme son nom l'indique, qu'un moyen de vérification. L'assurance que doit avoir le destinataire d'un message signé électroniquement porte sur la garantie que la signature électronique qu'il entend vérifier émane bien du signataire. Il ne peut avoir cette garantie que, notamment, par la vérification du lien entre le titulaire et sa clé publique, la clé privée devant, par nature, demeurer secrète.

18. ***Révocation du certificat*** - Pour de multiples raisons, il se pourrait que la confidentialité des données afférentes à la création de signature soit compromise ou que le titulaire du certificat craigne qu'il en soit ainsi. C'est pour parer à cette éventualité que la directive impose à tout PSC délivrant des certificats qualifiés ou garantissant publiquement de tels certificats, d'assurer le fonctionnement d'un service de révocation sûr et immédiat et de veiller à ce que la date et l'heure de révocation d'un certificat puissent être déterminées avec précision (Annexe II, c et d). La procédure de révocation vise donc à mettre fin à un certificat avant son terme. Par conséquent, le titulaire ne peut plus utiliser les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature certifiées dans le certificat révoqué pour générer une signature électronique. La responsabilité du PSC ne pourrait être engagée si le titulaire contrevenait à cette obligation.

19. Le régime de responsabilité établi par la directive tente de respecter un équilibre entre les intérêts des PSC et des utilisateurs de certificats afin que le niveau de certification mis en place présente un haut degré de fiabilité et, par là même, de crédibilité, sans qu'il n'entrave pour autant le commerce électronique. En vertu du régime mis en place, le PSC est donc responsable de tout préjudice causé à toute personne qui se fie légitimement au certificat, qui découle du manquement à une des obligations énumérées ci-dessus, sauf si elle prouve qu'elle n'a commis aucune négligence.

20. Le PSC peut toutefois limiter sa responsabilité. Deux types de clauses relatives à la responsabilité peuvent figurer sur le certificat qualifié. Le prestataire peut tout d'abord fixer des limites à l'utilisation du certificat. Dans cette hypothèse, il ne doit pas être tenu responsable du préjudice résultant de l'usage abusif du certificat qui contient ce type de clause. Il peut ensuite indiquer sur le certificat la valeur maximale des transactions pour lesquelles le certificat peut être utilisé.

Rappelons toutefois que les clauses relatives à la responsabilité doivent être appréciées de façon circonstanciée. Elles ne seront opposables aux personnes qui se fient légitimement aux certificats que si celles-ci en ont pris connaissance ou, à tout le moins, ont pu raisonnablement en prendre connaissance au plus tard au moment de la consultation du certificat. C'est la raison pour laquelle elles doivent obligatoirement figurer *sur le certificat*. En toute hypothèse, elles ne pourraient vider l'activité des tiers de confiance de son objet. Seraient considérées comme telles les clauses par lesquelles un tiers de confiance refuserait d'engager sa responsabilité quant à la véracité des informations fournies ou celles par lesquelles le PSC s'exonérerait de sa responsabilité pour le seul motif que la collecte des données a été confiée à une autorité d'enregistrement.

3.- La fiabilité comme fondement de la certification

21. Tout PSC qui désire émettre des *certificats qualifiés* doit se conformer aux prescriptions de l'annexe II de la directive. Des prescriptions sont également stipulées dans les annexes III et IV. Elles tendent à garantir la sécurité du mécanisme de certification. En effet, certaines garanties de base doivent impérativement être fournies par un PSC afin de créer et de renforcer la confiance que les utilisateurs peuvent avoir en lui.

22. ***Garanties de sécurité et de fiabilité*** - Le PSC doit « utiliser des systèmes et produits fiables » (annexe II, f). A cette fin, la Commission peut attribuer et publier au *Journal officiel des Communautés européennes* des numéros de référence de normes généralement admises pour des produits de signature électronique. Lorsqu'un produit est conforme à ces normes, le critère de fiabilité est présumé respecté.

Concernant les certificats, le PSC doit prendre les mesures nécessaires contre leur contrefaçon (annexe II, g). Pour cela, il doit notamment utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable de sorte que :

- *seules les personnes autorisées puissent introduire et modifier des données,*
- *l'information puisse être contrôlée quant à son authenticité,*
- *les certificats ne soient disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement et*
- *toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur* (annexe II, point l).

Lorsqu'il génère les données afférentes à la création de signature, le PSC doit garantir la confidentialité au cours de ce processus. Une fois ces données créées, il ne peut évidemment ni les stocker, ni les copier (annexe II, g et j).

Enfin, le PSC doit posséder l'expertise nécessaire pour assurer ses activités de certification. A cette fin, il emploie du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier, des connaissances en gestion et en technologie des signatures électroniques ainsi qu'une bonne pratique des procédures de sécurité appropriées (annexe II, e).

23. *Garanties d'information* - Rappelons que l'objectif de la directive est de renforcer la confiance et de promouvoir l'utilisation de la signature électronique avancée. L'information correcte de l'utilisateur des services contribue à la réalisation de cet objectif. Le PSC a donc l'obligation de procurer toute information nécessaire à l'utilisation correcte et sûre de ses services. Ces informations doivent être fournies dans une « langue aisément compréhensible ». De plus, elles doivent être fournies par un moyen de communication durable ou sur tout support durable. On vise par ces termes de nouvelles formes de communication susceptibles de remplacer l'écrit traditionnel. Ces nouvelles formes de communication peuvent valablement se substituer à un écrit pourvu que l'instrument utilisé présente des garanties de fiabilité suffisantes, et que son destinataire puisse prendre connaissance sans difficulté des informations ainsi diffusées. La proposition de directive

concernant la commercialisation à distance des services financiers[25] auprès des consommateurs définit la notion de support durable comme "tout instrument permettant au consommateur de conserver des informations, sans qu'il soit tenu de procéder lui même à l'enregistrement de ces informations ; sont notamment des supports durables au sens de cette directive les disquettes informatiques, les CD-ROM, ainsi que le disque dur de l'ordinateur du consommateur stockant des courriers électroniques ». Par ailleurs, la proposition de directive précitée insiste sur le fait que les données stockées sur support durable doivent être accessibles, c'est-à-dire que leur destinataire doit être en mesure d'en prendre connaissance aisément et de les conserver. On ne parlera donc pas de support durable si les informations sont communiquées par le biais d'une page web, spécialement s'il n'y a aucun téléchargement.

24. ***Garanties financières*** - Le PSC doit posséder des garanties financières suffisantes pour exercer ses activités et, le cas échéant, indemniser les utilisateurs ayant subi un dommage suite à l'inexécution des obligations qui lui sont imposées par ou en vertu de la directive. A cet effet, il devrait se couvrir par une assurance appropriée.

25. ***Garanties d'interopérabilité*** - Enfin, comme l'indique la Commission européenne dans sa communication du 8 octobre 1997[26] et dans le considérant numéro 5 de la directive, l'interopérabilité des différents systèmes et applications de signatures électroniques est absolument nécessaire afin d'assurer que celles-ci puissent être mises en œuvre en Europe et en dehors de l'Europe.

C.- Protection des données à caractère personnel

26. Le PSC qui est chargé d'établir un certificat doit être en mesure de vérifier de manière certaine et non équivoque le candidat titulaire. A cette fin, il est amené à collecter diverses informations sur les candidats. La directive impose aux Etats membres de veiller à ce qu'un PSC ne puisse recueillir de données personnelles que directement auprès de la personne concernée ou avec son consentement explicite et uniquement dans la mesure où cela est

[25] Proposition du Parlement européen et du Conseil du 19 novembre 1998 concernant la commercialisation à distance de services financiers auprès des consommateurs, modifiant les directives 90/619/CE, 97/7/CE et 98/27/CE, *J.O.C.E.* C du 11 novembre 1998 p. 385.

nécessaire à la délivrance et à la conservation du certificat (article 8.2). Ceci semble faire obstacle à ce que le PSC puisse accéder au registre national des personnes physiques, comme le prévoyait le premier projet de loi belge sur les autorités de certification, pour récolter ou vérifier ces données[27].

Le candidat titulaire n'étant pas légalement obligé ou ne désirant pas communiquer son identité, peut choisir un pseudonyme qui lui permettra de sauvegarder son anonymat. Ce droit à l'anonymat est consacré par la directive. En vertu de ce principe, les Etats membres ne peuvent empêcher le PSC d'indiquer dans le certificat un pseudonyme au lieu du nom du signataire (article 8.3).

D.- Reconnaissance transfrontière des certificats

27. Afin de revêtir une réelle utilité, toute infrastructure de certification doit être envisagée dans une perspective internationale. C'est pourquoi la directive requiert en son article 7 que les Etats membres traitent les certificats qualifiés par un PSC établi dans un pays tiers comme équivalents aux certificats délivrés par un PSC établi dans la Communauté européenne et ce, pourvu qu'une des conditions suivantes soit remplie :

1. le PSC remplit les conditions visées dans la directive et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un Etat membre ;
2. un PSC établi dans la Communauté, qui satisfait aux exigences de la directive, garantit le certificat ;
3. le certificat ou le PSC est reconnu dans le cadre d'un accord bilatéral ou multilatéral entre la Communauté et des pays tiers ou des organisations internationales.

Par cette disposition, la directive entend susciter la confiance des utilisateurs et ouvrir les portes au commerce international.

---

26 COM(97)503, *op. cit.*, p. 21.

27 Ce point a d'ailleurs été confirmé par le Conseil d'Etat : 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., 16 décembre 1999, n° 322, p. 57.

CONCLUSIONS

La directive sur un cadre communautaire pour les signatures électroniques ne s'est pas fait attendre. En adoptant le texte avant le « prétendu bogue de l'an 2000 », la Communauté européenne a démontré sa volonté d'avancer dans ce domaine.

En interdisant un système d'autorisation préalable, sans toutefois exclure les régimes volontaires d'accréditation, la directive adopte un principe, incontestable, qui se veut respectueux des règles de concurrence.

Concernant le régime juridique des PSC, la directive met sur pied un mécanisme de certification fiable et crédible, sans qu'il n'entrave pour autant le commerce électronique, en fixant de manière claire d'une part, la responsabilité des PSC, qui apparaît comme un juste équilibre entre les intérêts des PSC et les utilisateurs de certificats, d'autre part, les règles relatives à la protection des données à caractère personnel, et, enfin, les principes relatifs à la reconnaissance des certificats délivrés par des PSC établis dans des pays tiers.

Pour ce qui est des effets juridiques de la signature électronique, le double régime mis en place, dont l'interprétation permet de constater qu'il s'appuie sur nos concepts ancestraux de recevabilité, force probante et valeur probante, a le mérite d'ouvrir nos concepts aux nouvelles technologies plutôt que de les bouleverser. Par cette directive, la Commission a donc choisi la voie de la continuité.

Néanmoins, la directive ne semble pas avoir pris conscience de la portée de ces concepts et des conséquences de leur application. En dehors de toute accréditation, elle reconnaît à la signature électronique avancée la même force probante que celle qui est attachée à la signature manuscrite, alors qu'elle aurait du se limiter à sa recevabilité, laissant le soin au juge d'en apprécier la valeur probante. En permettant aux PSC de prétendre qu'ils respectent les exigences de l'annexe II en dehors de tout système d'accréditation, et en faisant bénéficier les signatures réalisées sur base de certificats émis par ceux-ci de la clause d'assimilation, la directive risque de manquer son objectif principal qui est de renforcer la sécurité et la confiance dans l'utilisation de la signature électronique.

On peut regretter que, comme prise de vertige par les bouleversements en cours, ou craignant porter atteinte au principe de la libre concurrence qui lui est si cher, la Commission ait privilégié ce dernier plutôt que la sécurité juridique. Là où il y avait défi, la Commission y a vu un choix.

Gageons toutefois que les Etats membres, plutôt que de réaliser une lecture exclusive des points 2 et 3 de l'article 3, en feront une lecture conjointe pour qu'ainsi, se fondant sur ces dispositions, ils maintiennent ou instaurent des régimes volontaires d'accréditation en vue non seulement d'améliorer le niveau de service fourni, mais également de contrôler les prestataires de service de certification établis sur leur territoire, délivrant des certificats qualifiés au public. Cet exercice n'est pas insurmontable, la Belgique vient d'en faire la preuve dans le projet de loi[28] qu'elle vient de déposer devant la Chambre …

Mireille ANTOINE
Didier GOBERT

[28] 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., 16 décembre 1999, n° 322.