La directive "Signature électronique" : la clé du commerce électronique ?

Antoine, Mireille

Published in:
Revue Ubiquité - Droit des Technologies de l'Information

Publication date:
2000

Document Version
le PDF de l'éditeur

La directive « signature électronique » : la clé du commerce électronique[1] ?

Mireille Antoine

L'essor du commerce électronique nécessite non seulement le développement de nouvelles techniques de signature, mais également leur reconnaissance juridique. Pour répondre à ces besoins, le Parlement européen et le Conseil ont adopté le 13 décembre 1999 une directive sur un cadre communautaire pour les signatures électroniques[2].

Cette directive poursuit deux objectifs majeurs. Le premier est la reconnaissance juridique des signatures électroniques (1.). Celles-ci ne pourront en effet favoriser le commerce électronique que si une valeur juridique leur est reconnue. Or dans la plupart des États membres, les exigences légales relatives à la preuve, et plus particulièrement à la signature, ne sont estimées satisfaites que pour la signature manuscrite. Pour atteindre l'objectif visé, la directive entend tout d'abord définir le concept de signature électronique (1.1.) pour ensuite réglementer ses effets juridiques (1.2.).

Le second objectif de la directive est de créer un cadre légal pour l'activité des prestataires de service de certification (2.). Après avoir fixé les principes d'accès au marché (2.1.), la directive pose les principes d'un mécanisme de certification fiable. Celui-ci s'articule autour de trois points essentiels : tout d'abord celui de la responsabilité des prestataires de service de certification, ci-après nommés PSC (2.2.), ensuite celui de la protection des données personnelles (2.3.), enfin celui de la reconnaissance, sous certaines conditions, de certificats délivrés par des PSC établis dans des pays tiers (2.4.).

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 États 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[3]. La Commission considère à ce propos que le principe de la liberté contractuelle doit prévaloir.

Chargée de recherches au CRID.

Cet article constitue une version condensée de l'article « La directive sur la signature électronique – Vers la sécurisation des transactions sur l'Internet ? », M. ANTOINE et D. GOBERT, *J.T.D.E.*, avril 2000, n° 68.

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.

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

1 Reconnaissance légale des signatures électroniques

1.1. Le concept de signature électronique

La directive entend tout d'abord promouvoir la reconnaissance légale des signatures électroniques. Afin de parvenir à une telle fin, diverses approches étaient possibles. Celle qui a été choisie pour la directive se fonde sur une approche fonctionnelle de la signature, rejoignant sur ce point la loi type sur le commerce électronique adoptée par la CNUDCI[4].

La directive définit la signature électronique comme étant « une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification » (art. 2.1.). Cette définition englobe un ensemble de techniques permettant la réalisation, par voie électronique, des fonctions de la signature classique, à savoir l'identification du signataire et sa manifestation de volonté d'adhérer au contenu du message auquel la signature se réfère. La directive opère une distinction entre ce terme générique de signature électronique et une technique plus spécifique de signature électronique qu'elle qualifie de « signature électronique avancée » (art. 2.2.). Est considérée comme telle, la 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 ;
d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

En choisissant le terme « signature électronique avancée », la directive choisit la voie de la neutralité technologique afin, d'une part, d'éviter que la proposition de directive devienne rapidement obsolète et, d'autre part, d'encourager la recherche et le développement de nouvelles techniques de signature. Toutefois, il ne fait pas de doute que, à l'heure actuelle, seule la technique de signature digitale ou numérique fondée sur la cryptographie asymétrique [5] répond à la définition de la signature électronique avancée donnée par la directive. Le contenu des annexes ne laisse planer aucun doute à ce sujet.

1.2. Effets juridiques de la signature électronique

Si la directive donne une définition de la signature électronique, elle entend également dans un second temps réglementer ses effets juridiques. Tel est l'objet de l'article 5 qui contient deux clauses : l'une d'assimilation et l'autre de non-discrimination.

Guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur le commerce électronique (1996), pp. 38 et 39.
Pour une description du fonctionnement de la signature digitales, voy. 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, 4/5, p. 292.

La clause d'assimilation (art. 5.1.) consiste à assimiler la signature électronique à la signature manuscrite, lorsque certaines conditions sont remplies[6], 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[7] 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).

La clause de non-discrimination (art. 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 États membres doivent veiller à ce que l'efficacité juridique[8] 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[9] 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[10].

Comme vu précédemment, la clause d'assimilation porte sur les signatures électroniques avancées basées sur un « certificat qualifié ». Même si cette notion est définie par la directive en son article 2, elle demeure ambiguë. Comment cette qualité est-elle reconnue à un certificat ? Comment avoir la certitude que le prestataire émettant ce certificat répond aux exigences de l'annexe 2 ? S'il paraît clair que les certificats émis par des PSC accrédités en vertu d'un régime mis en place dans les États membres répondent à cette définition, les autres cas où la qualité de certificat « qualifié » doit être reconnue aux certificats sont peu clairs. Est-ce une situation de fait, et il convient dès lors de vérifier que les conditions fixées par les deux annexes sont remplies pour avoir l'assurance que le certificat puisse être considéré comme qualifié, ou suffit-il qu'un PSC offre des certificats qu'il présente comme qualifiés, créant ainsi une apparence ?

Cette dernière hypothèse se dégage de l'article 6 qui traite des certificats « présentés comme agréés ». Elle est source de confusion et risque d'avoir d'énormes répercussions sur le plan de la responsabilité des prestataires de service de certification.

6. 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.
7. 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.
8. On peut s'interroger sur la signification concrète de ce concept « d'efficacité juridique » !
9. 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.
10. Sur les conséquences de la distinction recevabilité/valeur probante, 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*.

2 Création d'un cadre légal pour l'activité des prestataires de service de certification

2.1. Principes d'accès au marché

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 l'intervention de tierces parties qui pourront certifier le lien entre une personne et son dispositif de création de signature[11].

Le principe posé par la directive est celui de la liberté de fourniture des services de certification. Les États 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 États 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 (art. 3.2.). Les critères d'accréditation doivent dans ce cas être «objectifs, transparents, proportionnés et non discriminatoires».

D'autre part, les États membres doivent veiller à contrôler les PSC établis sur leur territoire délivrant des certificats qualifiés (art. 3.3.). Ce contrôle doit être effectué sur base des critères énumérés à l'annexe 2. Ceux-ci tendent à garantir la sécurité du mécanisme de certification. Ils doivent être respectés par tout PSC qui entend délivrer des certificats qualifiés et ce, pour créer et renforcer la confiance que les utilisateurs peuvent placer dans un mécanisme de certification.

En réalité, la directive ne revêt d'intérêt que si les États membres, se fondant sur les principes énoncés ci-dessus, mettent sur pied un régime d'accréditation, permettant un contrôle *a priori* des PSC[12]. 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[13], étant donné la difficulté d'apporter une telle preuve[14]. Or, elle semble envisageable en pratique.

11. 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.
12. 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.
13. Nous parlons ici de consommateurs car c'est effectivement en vue de la protection de leurs intérêts que les exigences formelles relatives à la conclusion des contrats ont été édictées.
14. 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.

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 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.

2.2. Responsabilité des PSC

En vertu de l'article 6.1. de la directive, le PSC qui délivre un certificat présenté comme qualifié ou qui garantit publiquement un tel certificat doit garantir :

- l'exactitude des informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié ;
- l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat ;
- dans le cas où le prestataire de service de certification génère les données afférentes à la création et à la vérification de signature, l'assurance que ces deux types de données puissent être utilisées de façon complémentaire (si l'on transfère ces exigences dans le contexte de la cryptographie asymétrique, cela reviendrait à dire que le PSC doit tester la complémentarité des clés privée et publique) ;
- la validité du certificat. Cet élément se dégage du point 2 de l'article 6 en vertu duquel le PSC doit être tenu responsable de tout préjudice causé à une personne qui se prévaut légitimement du certificat pour avoir omis de faire enregistrer la révocation dudit certificat.

Le PSC est responsable de tout préjudice causé à toute personne qui se fie légitimement au certificat et qui découle du manquement à une de ces obligations sauf s'il prouve qu'il n'a commis aucune négligence.

Le PSC peut limiter sa responsabilité. Deux types de clauses relatives à la responsabilité peuvent figurer sur le certificat qualifié. Le prestataire peut, soit fixer des limites à l'utilisation du certificat, soit indiquer dans le certificat la valeur limite des transactions pour lesquelles le certificat peut être utilisé. Le prestataire ne doit pas être tenu responsable du préjudice résultant de l'usage abusif du certificat qui contient des limites à son utilisation.

2.3. Protection des données à caractère personnel

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 États 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 nécessaire à la délivrance et à la

conservation du certificat (art. 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[15].

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 États membres ne peuvent empêcher le PSC d'indiquer dans le certificat un pseudonyme au lieu du nom du signataire (art. 8.3.).

2.4. Reconnaissance transfrontalière des certificats

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 États 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 :

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 État 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.

Conclusion

La directive sur un cadre commun pour les signatures électroniques constitue une avancée considérable dans le domaine du commerce électronique. Associée à la future directive «commerce électronique», elle sonne le glas d'un formalisme probatoire particulier en matière contractuelle. En effet, là où existent des exigences formelles relatives à la conclusion des contrats, il est demandé aux États membres de reconnaître que ces exigences puissent être adéquatement rencontrées par la signature électronique. À cet égard, la directive a le mérite d'ouvrir nos concepts ancestraux aux nouvelles technologies plutôt que de les bouleverser.

15. Ce point a d'ailleurs été confirmé par le Conseil d'État : 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.

Toutefois, la confiance dans un mécanisme de signature électronique repose sur un processus de certification fiable. En permettant aux PSC de prétendre qu'ils satisfont aux exigences de fiabilité édictées par l'annexe II de la directive en dehors de tout système d'accréditation, et en faisant bénéficier les signatures électroniques 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.

Il convient dès lors de considérer que la directive «signature électronique» n'est pas un aboutissement et qu'elle ne sera source de sécurisation du commerce électronique que si les États membres, réalisant une lecture conjointe des points 2 et 3 de l'article 3 de la directive, 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.

Telle est la clé d'accès à un commerce électronique sécurisé.