Signature électronique et autorités de certification

Gobert, Didier

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

Publication date:
1998

Document Version
le PDF de l'éditeur

Signature électronique et autorités de certification : la levée des obstacles au développement du commerce électronique[1]

Didier Gobert

(publié dans la revue *Ubiquité*, novembre 1998, n° 98/1, pp. 79-82.)

Le 12 juin 1998, le Conseil des ministres adoptait en première lecture deux avant-projets de loi[2] intimement liés au développement du commerce électronique : l'un visant à « modifier certaines dispositions du Code civil relatives à la preuve des obligations », l'autre relatif à « l'activité d'autorités de certification agréées en vue de l'utilisation de signatures digitales ». Ces deux textes constituent un grand pas en avant dans la levée de certains obstacles juridiques, et non des moindres, à la conclusion de transactions commerciales par les réseaux essentiellement ouverts, comme Internet.

Dans le monde et notamment dans notre pays, de plus en plus d'actes juridiques sont accomplis par voie électronique. Les technologies informatiques et des télécommunications créent, tant dans le secteur privé que dans le secteur public, des possibilités permettant de travailler plus vite et plus efficacement. Des contrats peuvent être conclus au moyen d'un ordinateur et ensuite être transmis pour approbation à l'autre contractant par le biais de réseaux, après quoi ils pourront être stockés sous une forme électronique. Ainsi, ils occuperont un espace d'archivage moins important et pourront être consultés plus rapidement.

Ces différentes transactions restent cependant limitées en raison de certains obstacles juridiques. D'une part, il est difficile, voire impossible, de prouver un grand nombre d'actes juridiques passés par voie électronique car la plupart des juges exigent encore un écrit papier signé manuscritement. D'autre part, trop peu de gens recourent aux autorités de certification en raison du manque de confiance essentiellement lié à l'absence de régime juridique relatifs à leurs activités. Les deux avant-projets de loi entendent mettre fin à cette incertitude juridique, néfaste au développement du commerce électronique. Notons que cette intervention législative n'est pas propre à la Belgique. L'Allemagne[3] et l'Italie[4] ont déjà adopté une loi dans ce domaine. Des projets de loi comparables sont en préparation dans d'autres Etats Membres (Pays-Bas, Luxembourg, Danemark, France)[5]. La question est également prise très au sérieux aux niveaux européen et international. En effet, la Commission européenne a adopté le 13 mai dernier une proposition de directive[6] sur un cadre commun pour les signatures électroniques et la Commission des Nations Unies pour le Droit Commercial

---

[1] Pour une étude approfondie du sujet, 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.*, septembre 1998, n° 4, pp.285 à 310.

[2] Ces deux avant-projets de loi ne sont pas encore publiés.

[3] http://www.iid.de/iukdg/iukdge.html

[4] http://www.aipa.it/english/law[2/pdecree51397.asp

[5] Vous trouverez les références dans les liens intéressants du site web du CRID à l'adresse suivante : http://www.droit.fundp.ac.be/liens/default.htm

[6] Vous trouverez la version française à l'adresse suivante : http://www.ispo.cec.be/eif/policy/com98297fr.doc. Pour un commentaire, voy. Rosa JULIA-BARCELO et Thomas C. VINJE, « Electronic signatures - another step towards a european framework for electronic signatures : the Commission's Directive proposal. », *C.L.S.R.*, 10/1998, n° 14/5, pp. 303-313.

International (CNUDCI) travaille sur l'élaboration de règles uniformes pour les signatures numériques[7].

Le premier avant-projet de loi vise à modifier les règles du Code civil afin qu'un document signé électroniquement ne puisse être rejeté d'office par le juge pour le seul motif qu'il se présente sous forme électronique. En effet, il dispose que peut, outre la signature manuscrite, également être considéré comme une signature « l'ensemble de données issues de la transformation de l'écrit et dont ressort avec certitude l'identité de l'auteur et son adhésion au contenu de l'écrit ». Cette approche, technologiquement neutre, permet d'ouvrir la définition aux mécanismes actuels et futurs de signature électronique tout en excluant ceux qui n'offrent pas un niveau de sécurité au moins équivalent à la signature manuscrite. Une autre disposition de l'avant-projet vise à permettre à tous les secteurs d'activité de procéder à un archivage électronique tout en se réservant des moyens de preuve. En effet, « est assimilé à un acte sous seing privé original l'écrit signé *(manuscritement ou électroniquement)* dont le maintien de l'intégrité du contenu est établi avec certitude ». Désormais, tant un document papier archivé soit sous forme papier soit sous forme électronique, qu'un document électronique archivé sous forme électronique seront considérés comme « originaux », pour autant que des mesures de sécurisation adéquates aient été prises afin de garantir leur intégrité[8].

Le deuxième avant-projet de loi est plus ciblé du point de vue technologique car il se limite à la technique de la signature digitale, basée sur la « cryptographie asymétrique »[9]. Cela s'explique par le fait que la signature digitale est pour l'instant le seul mécanisme de signature électronique fiable, ayant dépassé le stade expérimental et étant, de surcroît, d'un coût abordable. Par ailleurs, l'avant-projet règle essentiellement les activités des autorités de certification agréée, organismes tiers qui n'interviennent actuellement que dans le cadre de l'utilisation de la signature digitale.

La signature digitale est basée sur la cryptographie asymétrique, dite « à clé publique », dans laquelle une personne dispose de deux clés complémentaires : l'une, privée, qui doit rester secrète et l'autre, publique, qui peut être librement distribuée. L'exemple suivant en illustre le fonctionnement. Alice désire envoyer à Bernard un message signé de façon électronique. Pour cela, Alice va signer le message au moyen de sa clé privée et envoie le tout à Bernard. Ce dernier va vérifier la signature au moyen de la clé publique complémentaire d'Alice. S'il parvient à décoder le message, Bernard est assuré que l'intégrité de celui-ci n'a pas été compromise et que la signature a été réalisée avec la clé privée d'Alice. Il peut dès lors avoir la certitude qu'elle est l'auteur du message pour autant qu'une AC certifie que cette clé publique est bien celle d'Alice. Cette autorité va préalablement remplir cette fonction de certification au moyen d'un certificat digital dans lequel elle confirme le lien entre une personne (en l'occurrence Alice) et sa clé publique, après avoir vérifié scrupuleusement l'identité de la personne (Alice). Ce certificat pourra être consulté dans un registre électronique tenu par l'AC, accessible à tous et notamment à Bernard.

En raison de l'importance du rôle joué par l'AC et de la confiance que les utilisateurs doivent avoir en elle, l'avant-projet entend mettre en place un régime juridique clair applicable aux AC qui désirent s'y soumettre. L'objectif est d'ailleurs clairement exposé dans une de ses

---

[7] http://www.un.or.at/uncitral/fr-index.htm

[8] Sur ces questions, voy. E. DAVIO, « Preuve et certification sur Internet », *R.D.C.*, 1997, pp. 660 et suivantes.

[9] Sur ces questions, voy. E. DAVIO, « Questions de certification, Signature et cryptographie », in Internet face au droit, Cahiers du CRID, n°12, Bruxelles, Story Scientia, 1997, pp. 65 à 86 ; M. ANTOINE et D. GOBERT, *op.cit.*.

dispositions qui précise que « La présente loi fixe les conditions générales d'agréation des autorités de certification … ainsi que les règles à respecter par ces dernières et les utilisateurs de certificats afin de renforcer la sécurité et la confiance dans l'utilisation de la signature digitale ». Le système adopté tend à être suffisamment souple afin de répondre à la demande du marché tout en adoptant des critères stricts pour offrir un niveau de protection élevé.

Le texte met en place un système volontaire d'agréation, en conformité avec la proposition de directive européenne. Une AC n'a donc pas l'obligation de demander une agréation pour exercer ses activités de certification. Toutefois, si elle désire en obtenir une, elle devra répondre aux conditions prévues (indépendance, sécurité, garanties financières, interopérabilité). L'obtention de l'agréation a pour conséquence de soumettre l'AC agréée à la loi, et notamment au régime clair de responsabilité (contrairement aux AC qui ne demandent pas d'agréation).

On peut voir au moins trois bonnes raisons pour une AC de demander une agréation, et pour les utilisateurs de recourir à une AC agréée. Premièrement, l'agréation constituera aux yeux du public une espèce de « label de confiance ». Deuxièmement, une disposition de l'avant-projet établit un lien avec la nouvelle définition du Code civil en prévoyant qu'une signature digitale constitue une signature au sens de cette définition pour autant qu'elle soit réalisée sur base d'un certificat émis par une AC **agréée**. Troisièmement, on peut s'attendre à ce que de nombreuses lois particulières exigent que l'on passe par une AC **agréée** lorsque l'on utilise une signature digitale dans les relations avec l'administration, et ce en raison du niveau supérieur de sécurité.

Contrairement à la loi allemande, l'avant-projet permet à une AC de délivrer des certificats non seulement à des personnes physiques mais également à des personnes morales (de droit privé ou de droit public). On peut s'en réjouir car il est vrai que sur les réseaux, bon nombre d'entreprises s'identifient sous leur dénomination sociale ou leur nom commercial, par exemple le site web d'une société, sans référence aucune à une personne physique. Ces certificats « personne morale » seront également très utiles pour les sociétés recourant à la labellisation de leur site (garantie quant à l'existence du site et quant au respect, par exemple, de la loi sur les pratiques du commerce ou le respect de la vie privée). Si l'avant-projet reconnaît la certification des personnes morales, il est toutefois regrettable qu'il n'ait pas consacré le principe de la signature des personnes morales. Deux exemples illustrent les difficultés qu'une telle situation risque d'engendrer. On doute fort qu'un employé d'un secrétariat social, par exemple, accepte qu'on utilise sa clé privée et son certificat, et prenne ainsi la responsabilité, pour envoyer, en badge, des milliers de déclarations toutes les nuits. Dès lors, seuls la clé et le certificat du secrétariat social pourront convenir. Dans un autre registre, un consommateur qui commande des biens par Internet auprès d'une entreprise de grande distribution est bien plus intéressé à être assuré de l'existence et de l'identité de celle-ci, que celle de l'éventuelle personne physique qui contrôle le système informatique, puisqu'en définitive, c'est cette entreprise qui sera engagée juridiquement et financièrement. Malheureusement, le texte exclut ces scénarios et exige toujours que la signature identifie une personne physique. Mais le texte n'est-il pas après tout qu'au stade d'avant-projet ? Bien des choses peuvent encore changer…

Didier GOBERT
Assistant à la Faculté de droit de Namur
Chercheur au CRID