

Note sur la signature électronique

Maître Anissa BOUSSOFARA



1. La signature électronique dans la législation tunisienne

La signature électronique correspond à la transposition dans le monde numérique de la signature manuscrite. Il s'agit d'un mécanisme d'engagement fiable faisant appel à des techniques cryptographiques. L'engagement du signataire est irrévocable. Le document est inaltérable, il ne peut pas être modifié.

Ce procédé est prévu par le droit tunisien et sa validité est reconnue. Il exprime le consentement du signataire dans le cadre d'un contrat électronique.

Ainsi, l'article 453 alinéa 2 du Code des obligations (COC) et des contrats dispose que :

La signature consiste à opposer de la propre main du contractant un nom ou un signe spécial intégré à l'écrit auquel il se rapporte. Lorsque la signature est électronique, elle consiste en l'utilisation d'un procédé d'identification fiable garantissant le lien entre ladite signature et le document électronique auquel elle se rattache.

L'article 453 bis ajoute que :

Le document électronique est l'écrit composé d'un ensemble de lettres et chiffres ou autres signes numériques y compris celui qui est échangé par les moyens de communication à condition qu'il soit d'un contenu intelligible, et archivé sur un support électronique qui garantit sa lecture et sa consultation en cas de besoin. Le document électronique fait preuve comme acte sous seing privé s'il est conservé dans sa forme définitive par un procédé fiable et est renforcé par une signature électronique.

Il ressort de ces dispositions que la signature électronique a la même valeur juridique que la signature manuscrite, elle dispose donc des mêmes prérogatives et engage le consentement des signataires de la même façon.

La loi 2000-83 du 9 Août 2000 Relative aux Echanges et au Commerce Electroniques a posé les principes de la signature électronique et la procédure à suivre pour sa mise en œuvre.

Ainsi, l'article 5 dispose que :

Chaque personne désirant apposer sa signature électronique sur un document peut créer cette signature par un dispositif fiable dont les caractéristiques techniques seront fixées par arrêté du ministre chargé des télécommunications.

L'article 6 ajoute que :

Chaque personne utilisant un dispositif de signature électronique doit:

Prendre les précautions minimales qui seront fixées par l'arrêté prévue à l'article 5 de la présente loi, afin d'éviter toute utilisation illégitime des éléments de cryptage ou des équipements personnels relatifs à sa signature.

Informé le fournisseur des services de certification électronique de toute utilisation illégitime de sa signature.

Veiller à la véracité de toutes les données qu'elle a déclarées au fournisseur de services de certification électronique et à toute personne à qui il a demandé de se fier à sa signature.

Enfin, l'article 7 précise que :

En cas d'infraction aux engagements prévus à l'article 6 de la présente loi, le titulaire de la signature est responsable du préjudice causé à autrui.

L'arrêté prévu par l'article 5 de susmentionné concerne spécifiquement les fournisseurs de certification électronique. Il s'agit de l'arrêté du ministre des technologies de la communication du 19 juillet 2001, fixant les données techniques relatives aux certificats électroniques et leur fiabilité qui a été amendé par un arrêté du 21 février 2018, au sujet de la fixation des spécificités techniques du cachet électronique visible. Ce dernier permet d'assurer l'intégrité et l'authenticité des documents électroniques et papier en y apposant un code à barre. Il s'agit d'un niveau avancé de certification qui a été adopté par des institutions publiques concernant un certain nombre de documents (diplômes, attestation de travail par exemple) et qui peut également être adopté par les entreprises désireuses d'accéder à un niveau élevé de sécurisation de leurs actes.

2. La force probatoire du document électronique comportant une signature électronique

En vertu de l'article 453 bis du COC, le document électronique a la même force probatoire qu'un acte sous seing privé s'il est conservé dans sa forme définitive par un procédé fiable et est renforcé par une signature électronique. La conservation par un procédé fiable peut consister en plusieurs procédés : microfilm, microfiches, CD-ROM, carte à puce, clé-USB... Le législateur n'a pas prévu de liste, sûrement en raison des avancées technologiques de la matière, qui sont toujours en mouvement.

Le document électronique pourra alors avoir la valeur juridique de l'acte authentique conformément à l'article 449 du COC disposant que :

L'acte sous seing privé, reconnu par celui auquel on l'oppose, ou légalement tenu pour reconnu, fait la même foi que l'acte authentique, envers toutes personnes, des dispositions et énonciations qu'il renferme, dans les conditions énoncées aux articles 444 et 445 ci-dessus sauf en ce qui concerne la date, ainsi qu'il sera dit ci-après.

3. La procédure à suivre

En application de loi susmentionnée et de l'arrêté du ministre des technologies de la communication du 19 juillet 2001, l'opérateur souhaitant utiliser une signature électronique dans ses échanges et contrats doit être titulaire d'un certificat électronique permettant de valider le lien entre la signature électronique et son signataire.

Le certificat électronique est une pièce d'identité sur internet qui permet de conclure des contrats et des transactions électroniques. Le procédé technique de la certification assure une parfaite confiance dans la signature électronique en diminuant les risques de contrefaçon et de répudiation.

La notion de certification est liée au terme « tiers certificateur » ou « tiers de confiance », il a la fonction d'archivage des messages passant par lui et les parties peuvent y revenir en cas de différend ce qui leur procure une preuve. Le tiers est une autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer leur clé publique et leur certificat. Sa fonction est de formaliser un lien qui existe entre des personnes (physiques ou morales) et une paire de clés asymétriques et émet des certificats servant à l'identification du titulaire de la clé privée correspondant à la clé publique mentionnée dans le certificat pour la signature. Il gère des clés de chiffrement selon des conventions secrètes qui garantissent la sécurité de traitement de l'information. Ce tiers certificateur assure la confidentialité des messages, et le maintien des données de base des utilisateurs et la localisation des partenaires commerciaux et la vérification de l'enregistrement et l'horodation des transmissions et des réceptions des messages. Le tiers certificateur peut être assimilé au « notaire électronique »¹.

Le procédé technique de la certification assure une parfaite confiance dans la signature électronique en diminuant les risques de contrefaçon et de répudiation.

Le certificat est délivré par le fournisseur de services de certification électronique qui doit être muni d'une autorisation préalable de l'Agence nationale de certification électronique, placée sous tutelle du ministère des technologies de la communication et de l'économie numérique.

4. Validité des signatures électroniques délivrées à l'étranger

Dans le cadre d'un contrat conclu avec un partenaire qui appose une signature électronique, il faut vérifier la certification électronique de ce dernier afin de s'assurer de la fiabilité de sa signature électronique.

En outre, concernant les certifications établies dans des pays étranger, l'article 23 loi de la loi n°2000-83 du 9 août 2000 prévoit que:

¹ R.Essid, « La législation tunisienne en matière de document électronique : réalités et perspectives », Revue de la jurisprudence et de la législation, centre d'Etudes Juridiques et Judiciaires, n°7, juillet 2006, p.16.

« Les certificats délivrés par un fournisseur de services de certification électronique établi dans un pays étranger ont la même valeur que ceux délivrés par un fournisseur de services de certification électronique établie en Tunisie, si cet organisme est reconnu dans le cadre d'un accord de reconnaissance mutuelle conclu par l'agence nationale de certification électronique. »

Par conséquent il faudra s'assurer auprès de l'Agence nationale de certification électronique, placée sous tutelle du ministère des technologies de la communication et de l'économie numérique, que le fournisseur de services de certification électronique qui a fourni la signature électronique du contractant étranger est bien reconnu par un tel accord.

Tunis le 17 juin 2020