QUELLE EST LA VALIDITÉ JURIDIQUE DE LA SIGNATURE NUMÉRIQUE?

écrit par Yannick Lauwers | avril 5, 2023

Avec le règlement eIDAS[1], l'Europe a cherché à accroître la sécurité juridique et la confiance dans les transactions électroniques au sein du marché unique en fournissant une base commune pour une interaction électronique sécurisée entre les citoyens, les entreprises et les gouvernements.[2] Mais quelle est la validité juridique de votre signature numérique ?

Après tout, l'instauration d'une confiance dans l'environnement en ligne est essentielle au développement économique et social. A cause d'un manque de confiance, les consommateurs, les entreprises et les gouvernements hésitent à effectuer des transactions par voie électronique et à utiliser de nouveaux services.[3] L'Europe vise donc un marché unique numérique pleinement intégré qui facilite l'utilisation des services en ligne, en tendant particulièrement à faciliter l'identification et l'authentification électroniques sécurisées.[4] L'un des moyens pour y parvenir est la signature électronique.

Le règlement eIDAS distingue trois types de signatures électroniques légalement valables :

1. Signature électronique simple

Il s'agit de données sous forme électronique jointes ou liées logiquement à d'autres données sous forme électronique, et utilisées par le signataire pour signer.[5] Dans de nombreuses situations, c'est une alternative écologique, efficace et sûre à la signature manuscrite classique. Par exemple, il n'est plus nécessaire d'imprimer, de signer et d'envoyer un document par la poste. Cependant, elle ne garantit pas l'authenticité de la signature (à lire : certitude quant à l'identité du signataire) ou l'intégrité du document (à lire : vérification de toute modification du document).

Bien qu'une signature électronique simple ne soit pas assimilée à une signature

manuscrite, le signataire peut se prévaloir du principe de non-discrimination.[6] Ce principe signifie qu'un tribunal ne peut pas refuser la signature électronique du seul fait de sa nature électronique. Toutefois, cela ne signifie pas que ce type de signature électronique a la même valeur juridique qu'une signature manuscrite.

2. Signature électronique avancée

Il s'agit d'une signature électronique qui :

- est liée de manière unique au signataire (par exemple en lui attribuant un code/une clé privée unique) ;
- permet d'identifier le signataire (par exemple, au moyen d'un certificat d'identité) ;
- est créée avec des données de création de signatures électroniques que le signataire, avec un niveau de confiance élevé, peut utiliser sous son contrôle exclusif (par exemple, l'accès à une clé privée n'est possible qu'après un code PIN) ;
- et rend les modifications traçables par la suite (par exemple, audit-trail ou hashing).[7]

Une signature avancée nécessite donc un certain nombre de contrôles techniques qui démontrent l'authenticité de la signature et l'intégrité du document à signer. Elle offre ainsi plus de garanties d'authenticité et d'intégrité qu'une signature électronique ordinaire. Comme pour la signature électronique ordinaire, la signature électronique avancée n'est pas assimilée à une signature manuscrite, mais le signataire peut s'appuyer sur le principe de non-discrimination.[8]

3. Signature électronique qualifiée

Il s'agit d'une signature électronique avancée qui :

- est créée à l'aide d'un dispositif de création de signature électronique qualifié (par exemple, un logiciel et/ou un matériel configuré pour créer une signature électronique et qui répond à certaines exigences) ;

- est basée sur un certificat de signature électronique qualifié délivré par un prestataire de services de confiance qualifié (par exemple, un certificat de signature répondant à certaines exigences).[9]

Il s'agit d'une forme de signature techniquement complexe qui, par rapport aux signatures simples et avancées, offre juridiquement le plus de garanties en termes d'authenticité de la signature et d'intégrité du document signé. Le principal exemple de signature électronique qualifiée est la signature via l'eID ou via l'application Itsme.

Cette signature électronique est assimilée à une signature manuscrite. Cela signifie que la signature électronique qualifiée a les mêmes effets juridiques qu'une signature manuscrite.[10] La signature électronique qualifiée bénéficie également de l'effet du principe de non-discrimination. En outre, une signature électronique qualifiée est reconnue dans tous les autres États membres de l'Union européenne lorsqu'elle est basée sur un certificat de signature émis dans un État membre.[11]

Conclusion

Dans l'Union européenne, la validité d'une signature électronique au sens d'eIDAS est en principe reconnue. C'est aussi plus courant que vous ne le pensez. Pensez, par exemple, à l'utilisation d'un code PIN pour retirer de l'argent de votre banque ou à la signature de votre déclaration d'impôt numérique avec votre eID.

Mais tout comme une signature écrite classique peut être contestée, une partie pourra aussi toujours contester la validité d'une signature électronique. Nous vous recommandons donc – en fonction du contexte (formel/informel) dans lequel vous vous trouvez – d'invoquer une signature électronique simple, ou une signature avancée ou qualifiée.

Si vous avez des questions après avoir lu cet article, n'hésitez pas à nous contacter à l'adresse email joost.peeters@studio-legale.be ou par téléphone au 03

216 70 70.

[1] RÈGLEMENT (UE) N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

[2] Voir le considérant (2) du règlement eIDAS.

[3] Voir le considérant (1) du règlement eIDAS.

[4] Voir le considérant (5) du règlement eIDAS.

[5] Voir l'article 3.10 du règlement eIDAS.

[6] Voir l'article 25.1 du règlement eIDAS.

[7] Voir l'article 3.11 et l'article 26 du règlement eIDAS.

[8] Voir l'article 25.1 du règlement eIDAS.

[9] Voir l’article 3.12 du règlement eIDAS.

[10] Voir l’article 25.2 du règlement eIDAS.

[11] Voir l’article 25.3 du règlement eIDAS.