

Présentation du règlement européen eIDAS pour la confiance dans les transactions électroniques au sein du marché européen.

Nadia ANTONIN, présidente du groupe de travail « Commerce électronique » de l'Académie des Sciences commerciales

Mai 2017

1. Introduction

Le Parlement européen et le Conseil de l'Union européenne ont adopté le 23 juillet 2014, le règlement n° 910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS ».

Ce règlement, qui abroge la directive du 13 décembre 1999 sur la signature électronique, *« vise à susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur en fournissant un socle commun pour des interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques et en accroissant ainsi l'efficacité des services en ligne publics et privés, ainsi que de l'activité économique et du commerce électronique dans l'Union »* (article 2 du règlement).

Il instaure un cadre européen en matière d'identification électronique et des services de confiance, afin de faciliter l'émergence du marché unique numérique.

La réglementation sur les services de confiance est entrée en vigueur le 1er juillet 2016. L'obligation de reconnaissance mutuelle des identités électroniques (eID) s'appliquera à partir du second trimestre 2018.

2. Exposé des motifs du règlement eIDAS

• Le faible développement de la signature électronique

A l'ère du tout numérique, certains processus ont plus de mal à évoluer que d'autres. La signature électronique en est un exemple. En effet, malgré la reconnaissance de sa force probante, le marché des signatures électroniques a eu du mal à se développer en France et aujourd'hui encore de nombreuses entreprises continuent à utiliser une signature manuscrite même si elles ont dématérialisé la quasi-totalité de leur processus. Les principales causes avancées pour expliquer l'infortune de la signature électronique sont les suivantes :

- La complexité de la technologie Infrastructures à Clés Publiques (ICP) sur laquelle repose la signature électronique.
- L'absence d'interopérabilité technique aussi bien au niveau national que transfrontalier et de son corollaire.
- La mauvaise compréhension des moyens de la signature électronique.
- La problématique de l'archivage électronique.
- Les obstacles psychologiques et sociétaux avec la crainte de la fraude notamment.
- Les textes ne manquent pas, mais ils contiennent des recommandations plutôt que de véritables directives.

Le législateur européen, parfaitement conscient de la situation, avait pris très tôt des directives sur la signature électronique et sur le commerce électronique. Cela étant, la directive européenne du 13 décembre 1999 sur la signature électronique s'est avérée être, en pratique,

un échec en raison notamment des divergences nationales dans la transposition de ladite directive ainsi que dans les choix techniques effectués par les Etats membres qui n'ont pas permis une interopérabilité transfrontière des signatures électroniques.

- **La nécessité d'instaurer un climat de confiance dans l'environnement en ligne**

Comme le souligne l'article 1 du règlement, « *instaurer un climat de confiance dans l'environnement en ligne est essentiel au développement économique et social. En effet, si les consommateurs, les entreprises et les autorités publiques n'ont pas confiance, notamment en raison d'un sentiment d'insécurité juridique, ils hésiteront à effectuer des transactions par voie électronique et à adopter de nouveaux services* ».

En ce qui concerne le commerce électronique, le Parlement européen dans sa résolution du 21 septembre 2010 a souligné l'importance de la sécurité des services électroniques et invité la Commission européenne à mettre en place un portail des autorités européennes de validation afin entre autres d'accroître la sécurité des transactions réalisées via internet.

3. Les principales mesures du règlement

Le règlement eIDAS est essentiellement consacré à l'identification électronique et aux services de confiance.

- **Identification électronique**

Dans le cadre du règlement eIDAS, l'identification électronique consiste à utiliser des données d'identification personnelle sous une forme électronique, pour représenter de manière univoque une personne physique ou morale ou une personne physique représentant une personne morale.

Le règlement prévoit par ailleurs l'instauration d'un système de notification de « schéma d'identification électronique » (voir glossaire) par les Etats membres et trois niveaux de garantie pour les moyens d'identification électronique (voir glossaire) délivré dans le cadre d'un schéma d'identification électronique notifié : faible, substantiel et élevé. Le niveau de garantie faible offre un niveau de confiance limité sur l'identité du signataire ; il confirme uniquement que le signataire est propriétaire de l'adresse e-mail. Le niveau de garantie « substantiel » doit permettre de « *réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité* » tandis que le niveau de garantie « élevé » doit permettre « *d'empêcher l'utilisation abusive ou l'altération de l'identité* ».

Les moyens d'identification électronique peuvent être demandés par des personnes physiques ou morales, ou par des personnes physiques représentant des personnes morales.

En France, la Direction interministérielle du numérique et du système d'information et de communication de l'Etat (DINSIC) assure le rôle d'autorité nationale en matière d'identification électronique et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est garante de la sécurité pour le volet identification électronique.

- **Les services de confiance**

Le règlement eIDAS a également pour objectif d'instaurer un cadre juridique pour l'utilisation des services de confiance. Il prévoit des exigences pour les services de confiance relatifs à la signature électronique, au cachet électronique (voir glossaire), à l'horodatage

électronique (voir glossaire), à l'envoi recommandé électronique (voir glossaire) et à l'authentification de sites internet au moyen d'un certificat d'authentification de site internet.

Un service de confiance permet de garantir l'identité du signataire, l'intégrité du document signé ainsi que la manifestation du consentement du signataire quant au contenu des données électroniques ainsi signées.

Le règlement établit une distinction entre les services de confiance qualifiés (voir glossaire) et les services de confiance non qualifiés. Les services de confiance qualifiés peuvent bénéficier d'effets juridiques spécifiques précisés dans le règlement et sont assurés par des prestataires de services de confiance qualifiés (voir glossaire).

4. Quels sont les types de signatures électroniques définies par le règlement eIDAS ?

Le règlement eIDAS définit des signatures électroniques avancées (SEA) et des signatures électroniques qualifiées (SEQ). Ces signatures doivent permettre d'harmoniser la signature de documents dans tous les Etats membres de l'Union européenne.

- **Une signature électronique avancée** doit répondre à plusieurs exigences : être liée exclusivement au signataire ; permettre d'identifier le signataire ; être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.
- **Une signature électronique qualifiée** est une signature électronique avancée reposant sur un certificat qualifié (voir glossaire) et créée au moyen d'un dispositif sécurisé de création de signature électronique (voir glossaire).

5. Glossaire

Cachet électronique : signature apposée au nom d'une personne morale servant à garantir la provenance et l'intégrité d'un document.

Certificat d'authentification de site internet : attestation qui permet d'authentifier un site internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré.

Certificat qualifié : Certificat électronique répondant aux exigences de l'article 6 du décret du 30 mars 2001 relatif à la signature électronique et fourni par un prestataire de service de certification agréé.

Dispositif sécurisé de création de signature électronique : Dispositif de création de signature qui satisfait aux exigences fonctionnelles énoncées par la directive sur les signatures électroniques.

Note : Ce dispositif doit notamment garantir par des moyens techniques et appropriés que les données de création de signature électronique ne peuvent être utilisées qu'une seule fois et que leur confidentialité est assurée.

Horodatage électronique : action consistant à apposer à un fichier une date fiable pour garantir son existence à une date donnée et son intégrité.

Moyens d'identification électronique : outil permettant de s'identifier et de s'authentifier pour un service en ligne au moyen des données d'identification personnelle.

Prestataire de services de confiance qualifié : prestataire qui fournit un ou plusieurs services de confiance qualifiés et ayant obtenu de l'organe de contrôle le statut de qualifié.

Schéma d'identification électronique : système qui permet la délivrance de moyens d'identification électronique à des personnes physiques ou morales ou à des personnes physiques représentant des personnes morales.

Service d'envoi de recommandé électronique : service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée.

Service de confiance qualifié : service de confiance qui satisfait aux exigences du règlement eIDAS.