Identification électronique et services de confiance

Une Foire Aux Questions pour mieux comprendre les enjeux et les objectifs du nouveau Règlement eIDAS européen.

Enfin ! Le Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS) a été adopté le 4 avril par l'assemblée plénière du Parlement européen. Ce Règlement touche à des domaines aussi variés que l'identification, les signatures, les cachets, l'horodatage, les certificats ou les services d'envois recommandés électroniques... Il convient de rappeler brièvement les raisons qui ont conduit à ce Règlement, ce qu'il va changer et qu'il reste à faire. Plutôt que de rappeler de manière générale le contexte dans lequel s'inscrit ce Règlement, nous avons préféré présenter ces éléments sous forme de foire aux questions, ces questions nous ayant déjà été posées par ailleurs. D'autres questions relatives aux Prestataires de services de confiance ou aux moyens de contrôler l'effectivité des services de confiance ne seront pas traitées.

Pourquoi le Règlement eIDAS ?

La directive 1999/93/CE relative à la signature électronique devait introduire la signature et l'écrit électroniques comme moyen de nature à renforcer la confiance sur les réseaux numériques dans l'Union européenne. Mais à aucun moment, les transpositions et leur application n'y sont parvenues pleinement comme le met en exergue l'analyse d'impact accompagnant la proposition de Règlement et ce, parce que **les lois transposant la directive 1999/93/CE dans les législations des différents Etats membres étaient diverses et variées** et les exigences diffèrent d'un pays à l'autre et d'un service à l'autre : ce qui pouvait créer une **distorsion de concurrence entre les prestataires**, contraire à l'esprit même du Marché unique. L'harmonisation réalisée par le bas, n'a pas atteint les objectifs et les usages de la signature ne se sont que peu développés

De plus, **les technologies de l'information centrées sur la confiance ont évolué depuis 1999** (date d'adoption de la directive 1999/93/CE relative à la signature électronique). A l'époque, l'horodatage, les envois recommandés électroniques mais aussi certains usages du certificat n'existaient pas encore dans la pratique...

Une mise à jour et des évolutions semblaient donc nécessaires. C'est ce qui a conduit la Commission a publié une proposition de règlement le 4 juin 2012 [1].

Quel intérêt de recourir à la voie du Règlement ?

Un Règlement européen est **un instrument juridique directement applicable dans tous les Etats membres sans interprétation ni adaptation**. Il garantit une meilleure harmonisation et est par conséquent approprié pour atteindre les objectifs assignés au texte. Ce Règlement viendra donc remplacer **les différentes dispositions existantes**.

Quels sont les objectifs du Règlement eIDAS ?

Le Règlement a pour objectif premier *« d'assurer le bon fonctionnement du marché intérieur »* (art.1.1), c'est-à-dire de **rectifier la situation préoccupante issue de la directive 1999/93/CE**.

Il a également comme objectif *« d'atteindre un **niveau adéquat de sécurité des moyens d'identification électronique et des services de confiance** »* en :

- fixant *« les conditions dans lesquelles un Etat membre reconnaît les **moyens d'identification** électronique des personnes physiques et morales »* étatiques ;
- établissant des règles juridiques et techniques applicables aux services de confiance (art.1.1) [2].

Qu'en est-il concernant l'identification ?

L'identification en question (art.6 et s) a trait à la délivrance des moyens d'identification électronique relevant de la compétence nationale des Etats membres (ex : pièces d'identité sur support électronique). Chaque Etat membre peut décider de **notifier son système d'identification électronique** (art.7) **selon un niveau de garantie différent** (art.8). Ainsi, tout moyen d'identification électronique délivré dans un autre Etat membre figurant sur une liste publiée par la Commission européenne dans le Journal officiel de l'Union européenne pourra être utilisé pour accéder à un service en ligne lorsqu'une identification électronique est exigée en vertu de la législation nationale ou de pratiques administratives (art.9.2).

---

[1] Éric A. Caprioli, Pascal Agosti, *« La régulation du marché européen de la confiance numérique : enjeux et perspectives de la proposition de règlement européen sur l'identification électronique et les services de confiance »*, Comm. Com. électr. n° 2, février 2013, ét. 3.

[2] Sur le sujet, voir l'ouvrage récent : Éric A. Caprioli, *« Signature électronique et dématérialisation »*, éd. LexisNexis, 2014.

Le Règlement se concentre donc sur les approches transfrontalières de reconnaissance et d'acceptation mutuelle de l'identification électronique **étatique**. Les Etats devront toutefois être particulièrement vigilants quant à la sécurité du système d'identification notifié (art.10), toute atteinte à la sécurité ou toute mauvaise attribution du moyen d'identification à son titulaire légitime pouvant engager sa **responsabilité** envers toute personne morale ou physique (art.11).

Quels sont les services de confiance visés ?

Après de nombreuses discussions entourant le périmètre des services de confiance compris dans le Règlement, les services cibles – hors identification – sont les suivants :

- Les **signatures électroniques** (art. 25 et s), que ce soit dans le secteur privé ou public. Pour les signatures électroniques dans le secteur public (art. 26), les Etats membres ne peuvent exiger une signature plus sécurisée que la signature électronique qualifiée de la part de citoyens de l'Union européenne et en créant une hiérarchie des signatures pour ce secteur. De plus, le considérant 52 du Règlement intègre également la **signature électronique centralisée** («remote electronic signature»). Enfin, si elles sont qualifiées (SEQ), elles seront équivalentes aux signatures manuscrites (art. 25.2) étant précisé que l'efficacité juridique des signatures électroniques non qualifiées ne pourra être déniée au seul motif qu'elles sont sous forme électroniques ou qu'elles ne répondent pas aux exigences des SEQ ;
- Les **cachets électroniques**, «sceaux» (art. 34) propres à une personne morale garantissant l'origine et l'intégrité des données associées (sans manifestation du consentement contrairement à la signature). Ce sont des signatures «techniques» réalisées avec un certificat serveur ;
- L'**horodatage électronique** (art. 39), déjà prévu en droit français (décret n°2011-434), permet de garantir l'exactitude de la date et de l'heure indiquées et de l'intégrité des données auxquelles se rapportent cette date et cette heure ;
- Les **certificats d'authentification de sites Web** (art. 43) sont destinés à la sécurisation des échanges, utilisés par les sites marchands, et permettent de sécuriser la connexion ainsi établie entre un client et un serveur. Il s'agit d'un moyen efficace pour lutter contre le phishing ; l'utilisateur peut vérifier que le site sur lequel il se trouve est bien celui qui s'est authentifié ;
- Les **services d'envois recommandés électroniques** (art. 41), là encore insérés en droit français (art. 1369-8 du code civil et décret n°2011-144), bénéficient d'une *«présomption quant à l'intégrité des données, à l'envoi par l'expéditeur identifié et à la réception par le destinataire identifié des données et à l'exactitude de la date et de l'heure indiquées par le service d'envoi recommandé électronique qualifié concernant l'envoi et la réception»* ;
- Les **documents électroniques** (art. 44) dont l'efficacité juridique et la recevabilité comme preuves en justice ne peuvent être déniées au motif de leur forme électronique. Il ne s'agit que d'un rappel du principe de non discrimination médiatique issu de la loi type de la CNUDCI sur le commerce électronique de 1999 ainsi que dans les directives européennes de 1999 (signature électronique) et de 2000 (commerce électronique).

En outre, le texte établit des règles de responsabilité applicables aux prestataires de services de confiance (PSCo).

Qu'est-ce qui n'entre pas dans le champ du Règlement ?

Ce Règlement ne s'applique pas **aux systèmes dits fermés** (ex : cartes bancaires) et aux **accords entre parties** (convention sur la preuve) (art. 2). Cela signifie qu'il pourra être dérogé contractuellement aux dispositions du Règlement.

A quoi servent les qualifications de produits ou prestataires prévues dans le Règlement ?

Le Règlement fixe les règles des procédures de qualifications. Sans entrer dans le détail, le fait de disposer de services de confiance qualifiés constitue un sésame quant à **leur interopérabilité et leur acceptation au sein du Marché intérieur**. Dès lors, on peut estimer que la démarche - volontaire - de certains prestataires de services de confiance constituera une des conditions de la confiance ; la fiabilité de leurs pratiques ou de leurs produits étant reconnue dans chaque Etat membre de l'UE.

Quand entrera-t-il en vigueur ?

Le texte révisé sera soumis à l'approbation du prochain Parlement et ensuite du Conseil. Le Règlement pourra alors être publié au Journal officiel de l'Union européenne vraisemblablement **vers la fin de l'été ou à l'automne 2014**. L'entrée en vigueur du règlement eIDAS est prévue vingt jours après publication. Cependant, il ne sera applicable pour l'essentiel de ses dispositions qu'à compter de la **mi-2016**, à l'exception de certaines dispositions. Il en résultera que la directive européenne du 13 décembre 1999 sur les signatures électronique sera abrogée.

Que reste-t-il à attendre ?

Le Règlement contient des références à de nombreux **actes délégués** (pour compléter ou modifier *«certains éléments non essentiels d'un acte législatif»* – art. 290 Traité) et **d'exécution** (dans les cas où il est nécessaire de prévoir des conditions uniformes d'exécution d'actes de l'Union juridiquement contraignants) de la Commission.

La majorité des actes permettra si nécessaire, de désigner des normes dont le respect entrainera une présomption de conformité aux exigences du règlement. D'autres actes consisteront à définir si nécessaires des procédures applicables aux autorités publiques. Les actes obligatoires du règlement serviront à définir un cadre d'interopérabilité des moyens d'identification, un label de confiance pour les prestataires de services qualifiés, le format de la *«liste de confiance»* ou les formats de signature pour les signatures électroniques «publiques». En ce sens, la Commission européenne s'appuiera sur les normes techniques (European Norm – EN) obligatoirement applicables.

Ces règles juridiques et ces normes techniques ont pour but d'assurer la confiance numérique ainsi que la sécurité juridique pour tous les acteurs des transactions électroniques qui seront désormais sécurisées et admises dans tous les Etats membres. ■

Les auteurs

Eric A. CAPRIOLI,
Avocat à la Cour, Docteur en droit, Vice-Président du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN).

Pascal AGOSTI,
Avocat associé, Docteur en droit.