Principales évolutions du régime de la signature, du cachet et de la copie numériques

par Eric A. **Caprioli**
Avocat à la Cour, Docteur en droit, membre de la délégation française aux Nations unies
Pascal **Agosti**
Avocat associé, Docteur en droit

Le règlement 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 (eIDAS)[1] est entré en vigueur le 17 septembre 2014 et s'applique depuis le 1er juillet 2016[2] pour de nombreuses dispositions. En outre, l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations modifie le code civil est entrée en vigueur le 1er octobre 2016[3]. Si le règlement, instrument d'application directe en droit interne, est fondamental pour la confiance[4], les questions relatives à la preuve électronique contribuent également de la sécurité juridique. Les deux textes sont étroitement imbriqués. Le règlement propose aux acteurs du marché une véritable boîte à outils qu'ils sont libres de choisir en fonction du niveau de sécurité requis selon les usages en cause. Il concerne une palette de services électroniques : identification, signature, cachet, horodatage, certificats d'authentification de site *web*, documents ou envois recommandés. Concomitamment, il définit les conditions de cette confiance en s'appuyant sur le régime des prestataires de services de confiance (PSCo) et les modalités de leur contrôle.

Il est rappelé, tout d'abord, que l'application du règlement eIDAS est fondée sur les principes de liberté et de volonté des parties qui se manifestent d'une double manière :

- les parties peuvent décider d'appliquer le règlement ou de régir leurs relations sur la base d'accords contractuels (ex : convention d'échanges électroniques avec convention sur la preuve) conformément à l'article 2 du règlement ;
- les acteurs du marché peuvent décider de l'utilisation ou non des services de confiance qualifiés.

Les nouvelles dispositions du code civil sur la preuve se situent dans cette perspective : d'une part, l'article 1356 confirme la validité des contrats sur la preuve, sous réserve que les parties en aient la libre disposition[5] et l'article 1367 confère à la signature électronique qualifiée une présomption de fiabilité (comme l'ancien article 1316-4), ce qui autorise les parties à utiliser des signatures non-qualifiées (simples ou avancées). D'ailleurs, la plupart des décisions de jurisprudence rendues à propos de l'écrit et de la signature électroniques ont concerné des services non qualifiés.

Seuls la signature, le cachet électroniques et la copie numérique seront traités, sous l'angle de leur valeur à la fois juridique et probatoire.

> Le nouvel article 1356 du code civil confirme la validité des contrats sur la preuve, sous réserve que les parties en aient la libre disposition, et le nouvel article 1367 confère à la signature électronique qualifiée une présomption de fiabilité

Services de signature électronique

La signature électronique contribue à constituer l'écrit électronique. Son régime juridique résulte à la fois des dispositions du droit français (code civil) et de celles du règlement eIDAS.

En droit interne

L'écrit et la signature électronique dans le code civil

Depuis le 1er octobre 2016[6], l'article 1366 du code civil dispose : « L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ». Quant à l'article 1367, il énonce : « La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État. ». Par conséquent, l'écrit et la signature électroniques n'ont pas connu de changement notable[7].

En revanche, les conditions de fiabilité de la signature ne seront plus les mêmes et renverront au règlement

(1) JOUE, n° L 257, 28 août. V. sur le projet de règlement E. A. Caprioli, Signature électronique et dématérialisation, LexisNexis, 2014 ; Th. Piette Coudol, Une législation européenne pour la signature électronique : RLDI juill. 2012, n° 2838. ; E. A. Caprioli et P. 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, CCE févr. 2013. Étude 3 ; et sur le Règlement : P. Agosti, Commerce électronique, la confiance électronique, entre droit et technique, Expertises, déc. 2014, p. 416 s. ; D. Gobert, Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie, www.caprioli-avocats.com.

(2) La période de transition entre la directive 1999/93/CE du 13 décembre 1999 et le règlement eIDAS se terminera le 1er juillet 2020, date d'expiration du dernier certificat qualifié au sens de la directive. V. pour les autres dates d'entrée en vigueur, l'art. 52 du règlement.

(3) JO du 11 février 2016.

(4) E. A. Caprioli, Sécurité et confiance dans le commerce électronique, JCP 1998, I, 123.

(5) Art. 1356 : « Les contrats sur la preuve sont valables lorsqu'ils portent sur des droits dont les parties ont la libre disposition.

Néanmoins, ils ne peuvent contredire les présomptions irréfragables établies par la loi, ni modifier la foi attachée à l'aveu ou au serment. Ils ne peuvent davantage établir au profit de l'une des parties une présomption irréfragable. ».

(6) JO du 11 février 2016.

(7) La notion de « celui qui appose [*la signature*] » étant dans les faits compris comme étant « son auteur ».

eIDAS dans le cadre d'un décret en Conseil d'État qui remplacera le décret n° 2001-272 du 30 mars 2001 [8]. Ce texte déterminera les exigences de fiabilité de la signature électronique qualifiée bénéficiant de la présomption de fiabilité de la signature électronique. Ce décret devrait préciser, à l'instar de l'article 2 du décret du 30 mars 2001 et conformément à l'article 3-12 du règlement ce qu'il faut entendre par : « "signature électronique qualifiée", une signature électronique avancée, qui est créée à l'aide d'un dispositif de création de signature électronique qualifié et qui repose sur un certificat électronique qualifié de signature électronique ». Ce sont ces dispositions du règlement eIDAS que l'on retrouvera dans le code civil qui permettront de juger de la fiabilité d'une signature électronique et de bénéficier de la présomption attache à ladite présomption.

Solutions jurisprudentielles

Les décisions sur la preuve et la signature électronique démontrent que l'exigence de la signature électronique présumée fiable [9] comme prérequis à sa validité ne correspond pas à la réalité juridique et judiciaire. Ces solutions dégagées par les tribunaux seront identiques avec l'entrée en vigueur des dispositions du code civil le 1er octobre 2016.

Administration de la preuve

Ainsi, un arrêt de la cour d'appel de Nancy en date du 14 février 2013, infirmant un jugement du 12 décembre 2011 du tribunal d'instance d'Épinal, a mis en exergue l'importance du fichier de preuve dans la gestion des litiges liés à une transaction électronique, ainsi que les modalités relatives à l'admission de la preuve électronique devant un juge [10].
Les faits sont les suivants : pour la conclusion d'avenant de contrat de crédit *revolving* par voie électronique, une société de crédit avait consenti à un emprunteur un crédit renouvelable dont le montant avait été augmenté par deux avenants, un troisième ayant été souscrit par voie électronique. Après plusieurs échéances restées impayées, l'établissement de crédit assigna l'emprunteur en justice pour demander le remboursement des sommes et produisait pour justifier du dernier avenant le document « fichier de preuve de la transaction ». Le tribunal d'instance d'Épinal a écarté cet élément en affirmant que « le document « fichier de preuve de la transaction » est insuffisant pour s'assurer non seulement de l'engagement de Monsieur X puisqu'aucun élément de la prétendue signature électronique ne permet de faire le lien entre l'offre de prêt non signée et le document produit, en l'état simple fichier imprimé sans garantie d'authenticité, ni justification de la sécurisation employée ». En effet, il s'est avéré que la preuve avait été mal présentée au juge [11]. Sur la base de cette constatation, le tribunal d'instance jugeait l'action de la société de crédit forclose.
La cour d'appel de Nancy a infirmé le jugement en se fondant sur les dispositions de l'article 1316-4 du code civil et du décret n° 2001-272 du 30 mars 2001 relatives à la signature électronique. La Cour a relevé que la société de crédit « produit aux débats le fichier de preuve de la transaction émis par l'autorité de certification [...]. La mention du numéro de l'avenant sur le fichier de preuve permet de vérifier que c'est bien cet avenant qui a été signé électroniquement par M. X. Par conséquent, la preuve de la signature par M. X. de l'avenant du 4 septembre 2008 est rapportée, contrairement à ce qu'a jugé le tribunal. »
Ces éléments démontrent l'importance de l'administration de la preuve en justice. Notons ici que la signature électronique en question était une signature électronique à la volée fondée sur un certificat à usage unique, valable pour une session de temps relativement brève ou pour une seule transaction. Une fois l'opération ou la session de temps terminée, le certificat n'est plus valide et ne peut plus être utilisé. Il sera archivé avec le contrat signé dans un fichier de preuve contenant l'ensemble des données démontrant, qu'à un instant donné, la signature était valable et qu'elle a produit les effets juridiques escomptés (acceptation des termes du ou des documents contractuels et intégrité, validation des certificats utilisés, etc.).

Admission de la signature électronique simple

Tout écrit disposant d'une signature électronique simple est admissible devant les tribunaux au même titre qu'un écrit disposant d'une signature électronique qualifiée bénéficiant de la présomption de fiabilité, sous réserve de rapporter la preuve que les exigences de fiabilité sont respectées (identification de l'auteur et intégrité de l'acte), la différence se situant uniquement au niveau de la charge de la preuve.

Ainsi, dans le cadre du recouvrement de créances, plusieurs cours d'appel ont reconnu la valeur juridique de la signature électronique « simple » aux fins d'établir un pouvoir [12]. Selon la cour d'appel de Caen : « Il importe peu que les dispositions du décret du 30 mars 2001 n'aient pas été respectées dès lors qu'elles n'ont d'implication que sur la charge de la preuve, la fiabilité du procédé imposée par le décret (du 30 mars 2001) étant présumée jusqu'à preuve contraire, tandis que la signature électronique simple doit être démontrée par son auteur. » En l'espèce, la fiabilité de la signature électronique simple était rapportée par :
- Un procès-verbal de constat d'huissier de justice permettant de constater la fiabilité du processus permettant de signer un pouvoir en ligne ;
- et d'une attestation émanant du président de la société signataire du pouvoir attestant que son contrôleur financier était bien l'auteur du pouvoir et qu'il était habilité à le faire.

Au sujet d'un pouvoir électronique donné à un mandataire judiciaire, la cour d'appel de Nîmes, dans un arrêt du 1er octobre 2015, rappelle à nouveau que « le principe n'est pas qu'à défaut de respecter les exigences du décret la signature est sans valeur, mais seulement que la fiabilité du procédé n'est pas présumée ». La Cour confirme le jugement du tribunal de commerce d'Aubenas et la validité du pouvoir électronique qui répondait bien aux critères de fiabilité portant sur l'identification de son auteur et sur l'immutabi-

(8) Décr. n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, JO 31 mars. Comme le dit le rapport au président de la République (JO 11 févr. 2016), ce décret devra être modifié « pour préciser que la signature électronique présumée fiable, prévue par le code civil, est la signature « qualifiée » au sens du règlement ».

(9) À savoir jusqu'au 1er juill. 2016, la signature électronique sécurisée présumée fiable. À compter de cette date, ce sera la signature électronique qualifiée.

(10) V. E. Caprioli, Première décision sur la preuve et la signature électronique d'un contrat de crédit à la consommation, JCP n° 18, 2013, 497, p. 866 à 869 et CCE juin 2013. Étude 11, p. 13. D'autres décisions reprenant la même argumentation et où la signature électronique n'a pas été déniée, existent : Douai, 8e ch., 1re sect., 2 mai 2013, CCE 2014, comm. 22, note E. Caprioli.

(11) Sur la décision du tribunal d'instance d'Epinal, v. CCE 2013, comm. 47, note E. Caprioli

(12) V. Aix-en-Provence, 26 juin 2014, CCE 2014, comm. 90, note E. Caprioli ; v. égal. Caen, 5 mars 2015. n° 13/03009, CCE 2015, comm., note E. Caprioli.

lité de son contenu imposés par les dispositions de l'article 1316-1 du code civil, dès lors que le support de transmission électronique utilisé respecte les règles relatives à la souscription des contrats en ligne, par l'utilisation de codes sécurisés. On notera, en l'espèce, les mêmes exigences que pour la décision de Caen [13]. Plusieurs méthodes peuvent être retenues, variables en fonction des risques. Enfin, la Cour de cassation a eu à juger d'un cas où un individu déniait avoir signé électroniquement un bulletin d'adhésion à un contrat d'assurance complémentaire : « que le jugement retient que la demande d'adhésion sous forme électronique a été établie et conservée dans des conditions de nature à garantir son intégrité, que la signature a été identifiée par un procédé fiable garantissant le lien de la signature électronique avec l'acte auquel elle s'attache, et que la demande d'adhésion produite à l'audience porte mention de la délivrance de ce document par la plate-forme de contractualisation en ligne [...] permettant une identification et une authentification précise des signataires en date du 25 mai 2011 » et reconnaissant ainsi la valeur probatoire à la signature électronique simple [14].

Les niveaux de signature électronique dans le règlement eIDAS

Le règlement eIDAS prévoit trois niveaux de signatures électroniques qui seront envisagés tour à tour [15]. Observons que la notion d'écrit ne fait pas partie des sujets traités dans le règlement.

Signature électronique simple

Si la définition de la signature électronique simple dans le Règlement eIDAS est quasi-tautologique : « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer » [16] (sic) ; elle renvoie aux fonctionnalités énoncées dans code civil (identification de son auteur et manifestation du consentement) [17]. S'agissant maintenant de la signature électronique en particulier, selon la première phrase de l'alinéa 2 de l'article 1367 du code civil [18], il faut que le procédé d'identification de la signature électronique soit fiable – comme le rappelle la jurisprudence [19] - et qu'il garantisse le lien (logique) avec l'acte auquel elle s'attache.
Par conséquent, la signature électronique doit *a minima* permettre de disposer de l'identité du signataire (vérifiée ou déclarée de manière suffisamment fiable) et assurer l'intégrité du document (par le biais d'une signature numérique que l'on retrouve aussi dans le cachet électronique), mais sans toutefois se limiter à ce seul aspect dans la mesure où la signature permet également de manifester la volonté du signataire de consentir à l'acte.

De manière générale, cette signature électronique simple est utilisée pour des produits ou des marchés avec des conséquences juridiques ou financières de faible importance comme : opérations de caisse, adhésion à des conditions d'utilisation pour des sites de commerce électronique... Néanmoins, la jurisprudence récente a reconnu la validité de l'utilisation de ce type de signature dans des crédits à la consommation ou pour souscrire une assurance complémentaire santé.

Signature électronique avancée

La définition de la « signature électronique avancée » se retrouve à l'article 3.11 du règlement. Il s'agit d'« une signature électronique qui satisfait aux exigences énoncées à l'article 26 [*à savoir*] :
- a) être liée au signataire de manière univoque ;
- b) permettre d'identifier le signataire ;
- c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ;
- et d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable ».

Les différentes caractéristiques de la signature électronique avancée sont donc :
- **L'identification du signataire**

Cette identification peut être effectuée :
  - à distance en recourant à des pièces justificatives (ex : copie d'une pièce d'identité, facture EDF, etc.) que le signataire transmettra par voie postale ou électronique. Celles-ci peuvent être vérifiées de manière plus ou moins poussée (en allant du simple contrôle de cohérence des pièces à un *scoring* de leur vraisemblance/pertinence) ;
  - en face à face lors d'une rencontre présentielle avec un représentant (autorité d'enregistrement, bureau d'enregistrement [20]) du prestataire de services de confiance [21] avec une vérification d'identité à partir d'une pièce d'identité valide.
- **Le lien univoque avec le signataire**

Ce lien univoque est assuré par l'émission d'un certificat entendu comme « une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne » [22]. Le certificat en question peut être un certificat à usage unique ou un certificat standard, c'est-à-dire qui pourra être réutilisable dans le temps pendant une période pouvant aller d'un à trois ans.
- **L'utilisation sous le contrôle exclusif du signataire de données de création de signature**

Le contrôle exclusif des moyens de création de signature constituait un obstacle au déploiement de la signature électronique sécurisée au motif de la nécessité pour tous de disposer d'un support cryptographique (carte, clé USB sécurisée, etc.) et du moyen de la mettre en œuvre. Le système était complexe et lourd à implémenter. Finalement, un groupe d'experts techniques s'est penché sur la question [23].
Deux niveaux de contrôle exclusif ont été identifiés :
  - « *Sole Control Assurance Level 1 : the signato-*

(13) V. Nîmes, 1er oct. 2015, CCE 2016, comm. 20, note E. Caprioli. V. aussi en ce sens Toulouse, 3e ch., 9 déc. 2015, n° 15/01828, *SA TKB c/ SARL Chevalier Diffusion.*

(14) Civ. 1re, 6 avr. 2016, n° 15-10.732, Inédit, JCP 2016, 783, note E. Caprioli.

(15) Art. 3.

(16) Art. 3.10.

(17) D'après I. Dauriac : « la fonction d'identification n'est pas une fonction probatoire mais une fonction symbolique. », La signature, Thèse Paris II, 1997, v. n° 182.

(18) Repris de l'ancien article 1316-4 du code civil.

(19) En ce sens, à propos d'une signature scannée (non admise) pour la signature d'une déclaration d'appel, Besançon, 20 oct. 2000, JCP 2001, II, 10606, p. 1890 s., note Eric A. Caprioli et Pascal Agosti ; confirmé par Civ. 2e, 30 avr. 2003, n° 00-46.467, Bull. civ. II, n° 118.

(20) Sur les questions d'enregistrement voir V. Eric A. Caprioli, De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ?, article disponible à l'adresse http://www.uncitral.org/pdf/english/colloquia/EC/Caprioli_Article.pdf et sur le site www.cprioli-avocats.com.

(21) Défini comme « une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié » (art. 3.19).

(22) art. 3.14.

(23) V. ainsi les travaux du CENT/TC 224 concernant la norme TS 14167, Chapitre 5 : « *Security Requirements for Trustworthy Systems Supporting Server Signing* », déc. 2014.

ry authentication is not enforced by the Signature Creation Device but by the Trusted Signature Creation Module environment and the Signature Creation Application uses the signatory's Signature Creation Device linked by the Trusted Signature Creation Module to the authenticated identity of the signatory ; it is not expected that such implementations would meet the requirements of sole control as it would be expected for an Secure Signature Creation Device ;

- *Sole Control Assurance Level 2 : the signatory authentication is enforced by the Signature Creation Device by a means that the signatory uses for signing (the Signature Activation Data) in order to enable the use of the corresponding Signature Creation Data ; the signatory authentication is aimed to achieve the same sole control assurance level as what would be achieved by a stand-alone Secure Signature Creation Device* » [24].

Si le premier niveau assure que seule l'utilisation des moyens de création de signature électronique est sous le contrôle exclusif du signataire, le second niveau assure que lesdits moyens restent maintenus sous le même contrôle exclusif [25].

Dès lors, les signatures électroniques avancées peuvent être soit établies à la volée soit centralisées comme le permet le considérant 52 du règlement eIDAS [26].

- **La garantie du lien entre l'acte et la signature électronique avancée**

La technologie mise en œuvre par le PSCo [27] doit assurer l'intégrité de l'acte, fonction assurée par l'établissement d'un lien logique entre l'acte et la signature par le biais de mécanismes cryptographiques [28].

La fiabilité de ce type de signature électronique doit être également rapportée par le demandeur, même si le niveau de sécurité juridique et technique est élevé grâce au respect de certaines normes techniques [29] vis-à-vis d'une signature électronique simple.

Notons que la signature électronique avancée peut être utilisée avantageusement dans une optique de déploiement national pour des produits financiers comme le contrat de crédit à la consommation, le contrat d'assurance, le contrat d'ouverture de compte ou le contrat de crédit immobilier… Mais, comme on l'a vu , la jurisprudence a également reconnu la valeur juridique de la signature électronique simple pour de tels cas d'usage.
Il en ira de même pour bon nombre de contrats souscrits électroniquement, mais avec la présence physique du client (agence, point de vente, etc.).

Signature électronique qualifiée

La signature électronique qualifiée, définie à l'article 3.12 du règlement [31] doit être considérée comme le fondement juridique et technique de l'interopérabilité dans le marché européen de la confiance [32]. En effet, si le règlement fixe les effets de la signature électronique de manière générale, affirmant que « L'efficacité juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée » [33], seule la signature électronique qualifiée est dotée d'un effet juridique « équivalent à celui d'une signature manuscrite » [34].

> La signature électronique qualifiée doit être considérée comme le fondement juridique et technique de l'interopérabilité dans le marché européen de la confiance

Cela ne signifie pas pour autant que le recours à une signature électronique qualifiée dispenserait le signataire de rapporter la preuve lors d'une vérification d'écriture [35] : elle serait – comme les signatures manuscrites – soumise aux articles 287 et 288-1 du code de procédure civile.

Cela étant, « l'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée. ».

Pour disposer d'une signature électronique qualifiée, les PSCo – eux-mêmes qualifiés – devront émettre des certificats qualifiés au sens de l'annexe 1 du règlement eIDAS. De plus, les dispositifs de création de signature devront eux aussi être qualifiés. Pour l'heure, la décision d'exécution n° 2016-650 du 25 avril 2016 est venue indiquer les normes applicables pour les dispositifs de création de signature électronique qualifiés « lorsque les données de création de signature électronique ou de cachet électronique sont conservées dans un environnement dont l'utilisateur a la gestion totale, mais pas nécessairement exclusive » [36].

(24) § 5.4 du document préc.

(25) § 5.4 du document préc.

(26) « La création de signatures électroniques à distance, système dans lequel l'environnement de création de signatures électroniques est géré par un prestataire de services de confiance au nom du signataire, est appelée à se développer en raison de ses multiples avantages économiques. Toutefois, afin que ces signatures électroniques reçoivent la même reconnaissance juridique que les signatures électroniques créées avec un environnement entièrement géré par l'utilisateur, les prestataires offrant des services de signature électronique à distance devraient appliquer des procédures de sécurité spécifiques en matière de gestion et d'administration et utiliser des systèmes et des produits fiables, notamment des canaux de communication électronique sécurisés, afin de garantir que l'environnement de création de signatures électroniques est fiable et qu'il est utilisé sous le contrôle exclusif du signataire. Dans le cas de la création d'une signature électronique qualifiée à l'aide d'un dispositif de création de signature électronique à distance, les exigences applicables aux prestataires de services de confiance qualifiés énoncées dans le présent règlement devraient s'appliquer. ».

(27) Prestataires de services de confiance.

(28) Avec la signature numérique, les utilisateurs ont la garantie des fonctions de sécurité mises en œuvre : l'authentification, l'intégrité, la confidentialité (si l'acte est chiffré) et la non-répudiation (fonction technique et non une fonction juridique).

(29) Comme par exemple les normes techniques Électronic Signatures and Infrastructures (ESI) ; *Policy and security requirements for Trust Service Providers issuing certificates* ; ETSI TS 319 411 (LCP ou QCP) et les standards techniques de l'ETSI TS 102 142 (pour le respect des procédures d'enregistrement).

(30) V. *supra*.

(31) V. *supra*.

(32) E. A. Caprioli et P. 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 : CCE févr. 2013. Étude 3. P. Agosti, Commerce électronique, la confiance électronique, entre droit et technique, Expertises, déc. 2014, p. 416 s.

(33) Art. 25-1.

(34) Art. 25-2.

(35) E A. Caprioli, La sincérité de la signature électronique, *in* La sincérité en droit, (sous la coordination de Olivier Le Bot), Bruxelles, Larcier, 2011, v. p. 111-127 ; disponible à l'adresse : http://www.caprioli-avocats.com.

(36) D'autres actes d'exécution sont donc à prévoir au sujet des dispositifs de création de signature électronique qualifié. Décision n° 2016/650 de la Commission du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, JOUE, L. 109, 26 avr.

Une autre décision d'exécution n° 2015/1506 de la Commission du 8 septembre 2015 établit les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur [37].
En outre, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié sur son site des référentiels juridiques pour que les PSCo puissent adapter leurs offres de services de confiance (dont notamment la signature électronique) au contexte du règlement eIDAS. Si certains référentiels (certification à la conformité au règlement eIDAS) sont d'ores et déjà stabilisés [38], d'autres nécessitent encore le retour du marché [39].
Allant au-delà des dispositions existantes, le règlement eIDAS prévoit également les conditions entourant la vérification [40] et la conservation des signatures électroniques qualifiées [41]. Ces normes seront applicables dans le cadre du code civil.

Le recours à la signature électronique qualifiée s'inscrit donc dans une optique européenne, pour les États membres, que ce soit :
– pour des actes graves comme les actes authentiques (notaires, huissiers de justice, décisions de justice) ou les actes juridiques d'avocats ; ou
– pour le déploiement d'une offre de services à l'échelle européenne, sans avoir à redouter une législation nationale contraire au règlement eIDAS et dont les effets juridiques seraient reconnus.

Services de cachet électronique

Fondé sur le même principe technique que la signature électronique, le règlement eIDAS a introduit le cachet électronique [42], ou « sceau numérique » propre à une personne morale garantissant l'origine et l'intégrité des données associées (sans manifestation du consentement contrairement à la signature) [43]. Ces nouveaux services ne figurent pas encore dans le code civil. Ce ne sont pas des signatures au sens juridique, mais des signatures « techniques » vérifiées à l'aide d'un certificat serveur. Elles seront utilisées pour valider juridiquement une multitude de documents (factures, bulletin de paie, proposition de contrat en ligne, etc.), échanges ou transactions électroniques au même titre qu'une signature par griffe au sens commercial du terme. Le considérant 59 du règlement précise les deux fonctions juridiques des cachets électroniques : ils « devraient servir à prouver qu'un document électronique a été délivré par une personne morale en garantissant l'origine et l'intégrité du document. » À l'instar de la signature électronique qualifiée, le cachet électronique qualifié répond à des exigences techniques et à des formats. La même décision d'exécution n° 2015/1506 de la Commission du 8 septembre 2015 [44] s'applique aux formats de cachet électronique dans le secteur public.
Le cachet électronique bénéficie d'une présomption de fiabilité (intégrité et exactitude de l'origine des données) contrairement au cachet électronique simple dont l'effet juridique et la recevabilité ne peuvent être refusés en raison de son caractère électronique ou qu'il ne répond pas aux exigences du cachet électronique qualifié. Cependant, celui qui se prévaut du cachet, devra établir sa fiabilité.

Les copies numériques

Ce volet de la preuve n'existe pas dans le cadre du règlement eIDAS ; il relève de la compétence des États membres. Compte tenu du développement des pratiques tendant à supprimer les originaux papier au bénéfice de copies numérisées, le gouvernement a souhaité apporter une certaine sécurité juridique en la matière et éviter aux acteurs économiques de cumuler deux formes d'archivage (un papier, l'autre digital). L'ordonnance n° 2016-131 du 10 février 2016 reconnaît ainsi la « copie fiable » et lui attribue la même force probante qu'un original.
L'article 1379 nouveau du code civil dispose : « La copie fiable a la même force probante que l'original. La fiabilité est laissée à l'appréciation du juge. Néanmoins est réputée fiable la copie exécutoire ou authentique d'un écrit authentique.
Est présumée fiable jusqu'à preuve du contraire toute copie résultant d'une reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par décret en Conseil d'État.
Si l'original subsiste, sa présentation peut toujours être exigée. ».
En conséquence, la reconnaissance de la force probante d'une copie à l'identique de celle d'un original est posée sous réserve que la copie soit fiable.
De plus, comme le souligne le rapport au président de la République, la destruction des originaux papier est désormais consacrée [45].
Il est très important de noter que la fiabilité de la copie est laissée à l'appréciation du juge. Ainsi, en matière judiciaire, ce sont donc les juges qu'il faudra convaincre de la fiabilité de la copie produite. Plus généralement, il appartient aux juges du fond de qualifier de « fiable » une copie à l'instar de celles qui devaient être considérées comme « fidèles et durables » en vertu de l'ancien article 1348, alinéa 2, du code civil, car il leur incombe d'en apprécier « souverainement la valeur et la portée » [46]. La fiabilité des procédés techniques de copies utilisés devra donc leur être rapportée (ainsi qu'aux experts qu'ils nommeront le cas échéant). En outre, les décisions rendues sous l'empire des anciens articles du code civil offrent des pistes quant aux critères attendus pour qu'une

(37) JOUE, L. 235, 9 sept.
(38) Pour ce qui concernent les dispositifs de création de signature électronique qualifiés : http://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/documents-publies-par-lanssi/.
(39) Pour ce qui concernent la validation des signatures électroniques qualifiées (mais aussi les cachets) : http://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/documents-publies-par-lanssi/ où un appel à commentaire était ouvert jusqu'à sept. 2016.
(40) Art. 33.
(41) Art. 34.
(42) Art. 34. L'art. 3.25 du Règlement eIDAS définit le cachet comme : « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières ».
(43) Sur la signature électronique de la personne morale, v. E. Caprioli, L'agent électronique et le contrat, in Les deuxièmes journées internationales du commerce électronique, Paris, Litec, 2003, v. p. 215-242 (spéc. p. 230 s.) et V. Eric A. Caprioli, De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ?, article disponible à l'adresse http://www.uncitral.org/pdf/english/colloquia/EC/Caprioli_Article.pdf (févr. 2011).
(44) JOUE, L. 235, du 9 sept
(45) Le rapport au Président de la République indique en commentaire des copies (article 1379) que « peu important que celui-ci (l'original) subsiste ou pas, et peu important l'origine, le cas échéant de la disparition de l'original. »
(46) Civ. 1re, 30 mai 2000, n° 98-16519.

copie soit considérée « fiable »[47], ce qui sous-entend que l'original papier a été détruit, puisque la fidélité et la durabilité participent à la fiabilité de la copie ainsi que le respect des spécifications de la norme AFNOR Z 42-013 « Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes ».

Ces éléments étant précisés, il convient d'analyser le régime juridique de la présomption de fiabilité de la copie[48]. D'une part, elle bénéficie d'une présomption irréfragable de par la loi selon l'auteur de la copie (officier public – copie exécutoire, ou authentique). D'autre part, la copie bénéficie d'une présomption simple de fiabilité dès lors qu'elle respecte les exigences relatives à la reproduction à l'identique de la forme et du contenu et de l'intégrité) qui seront définies par un décret en Conseil d'État. À cet égard, ledit décret devrait fortement s'inspirer de la norme AFNOR Z42-013 sur laquelle les décisions jurisprudentielles précédemment citées se sont fondées. Alors que la preuve contraire pourra toujours être rapportée, il reste que l'archivage électronique des copies numériques représente un enjeu majeur pour les entreprises étant donné que cet usage est déjà largement répandu, notamment avec des solutions de gestion électroniques des documents (GED) et de numérisation.

Finalement, force est de constater que l'évolution des technologies et leur diffusion imposent une modification sensible des usages des services de confiance avec de nouveaux services et normes techniques. D'un autre côté, les techniques de reproduction et de numérisation ne pouvaient rester en l'état et la modification du code civil répond à une nécessité. Et l'ensemble du processus de digitalisation des organisations privées (et publiques) pourra s'appuyer sur ces nouveaux textes, inscrits pour être en phase avec le progrès technologique. Mais jusqu'à quand ?

(47) CA Paris, 11 févr. 2016, n° 15/01765, CCE 2016, com. 47, note E. Caprioli ; Lyon, 3 sept. 2015, n° 13/09407, CCE 2015, comm. 95, note E Caprioli. Lyon 4 juill. 2014, n° 13/02989, Inédit ; Paris, 5 mars 2015, n° 14/11341, Inédit ; Douai 4 avr. 2013, n° 12/02039, Inédit ; ces décisions ont été rendues en matière bancaire.

(48) À toutes fins utiles, il est également précisé que l'article 1354 nouveau du code civil détermine : « La présomption que la loi attache à certains actes ou à certains faits en les tenant pour certains dispense celui au profit duquel elle existe d'en rapporter la preuve.

Elle est dite simple, lorsque la loi réserve la preuve contraire, et peut alors être renversée par tout moyen de preuve ; elle est dite mixte, lorsque la loi limite les moyens par lesquels elle peut être renversée ou l'objet sur lequel elle peut être renversée ; elle est dite irréfragable lorsqu'elle ne peut être renversée. ».