➜ ACTUALITÉS

Affaires

INTERNET

28

Le décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique

POINTS-CLÉS ➜ La présomption de preuve littérale de l'écrit électronique renvoie à la signature qualifiée ➜ Le règlement e-IDAS vise à harmoniser les conditions de la signature qualifiée ➜ La réglementation française est donc remise en question ➜ Le jeu de la présomption du droit français n'en sera pas facilité à tous égards.

Anne Penneau
professeur de droit privé, faculté de Droit Sciences Politiques et Sociales, université de Paris 13 - Sorbonne Paris Cité - IRDA

1. - De la réglementation nationale à la réglementation européenne. - La loi du 13 mars 2000, qui a transposé la directive européenne 1999/93 sur la signature électronique en créant un régime légal de la preuve de l'écrit électronique, dans l'ancien article 1316-4 du Code civil, a pour la première fois dans l'histoire du Code civil, opéré un renvoi à la réglementation, en en faisant même la clé de voûte du système probatoire de l'écrit électronique : établi conformément au décret pris en Conseil d'État, un écrit électronique est présumé valoir preuve littérale.

Par le fait de conditions drastiques de la signature sécurisée inscrites dans le décret n° 2001-272 du 30 mars 2001, il était voulu que ladite présomption – de nature réfragable – ne risque pas d'être en pratique écartée. Et c'est dans le même sens que des réglementations complémentaires (*D. n° 2002-535, 18 avr. 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information : JO 19 avr. 2002, p. 6944 ; A. 26 juill. 2004 relatif à la reconnaissance de la qualification des services de certification et à l'accréditation des organismes qui procèdent à leur évaluation : JO 7 août 2004, p. 14104*) ont régi, d'une part, l'organisation des *process* dédiés à l'évaluation et la certification de la sécurisation des dispositifs de signature électronique utilisés pour établir l'acte électronique (logiciels sur disque dur, clé USB…), et, d'autre part, les conditions de délivrance des certificats électroniques dont la fonction est d'identifier celui qui signe électroniquement par un système de clé publique associée à une clé privée dont il doit conserver le secret.

Le résultat de cette orientation réglementaire a, en réalité, été de rendre inatteignables en pratique les conditions techniques propres à déclencher la présomption. En fonction de quoi le droit positif s'est finalement développé en large partie hors de l'emprise de la réglementation (*A. Penneau, La preuve des actes électroniques en droit français - Conséquences du règlement européen e-IDAS : JCP E 2017, 1264 et les réf. citées*). Écartant le jeu de la présomption par une application rigoureuse de ces conditions, les juridictions de l'ordre judiciaire aussi bien qu'administratif n'en ont pas moins largement reconnu la valeur probatoire de toutes sortes d'écrits électroniques (fichiers numériques, courriels, SMS) en tant qu'actes juridiques (*ibid*). Cependant que les pratiques de l'e-administration ont tendu à s'appuyer sur une interprétation minimaliste de la réglementation.

Face à la diversité des droits des États membres et prioritairement animée par la volonté d'harmoniser les pratiques d'e-administration liées à diverses facettes de la libre circulation, l'Union européenne a remplacé la directive 1999/93 par un 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 (e-IDAS) (*PE et Cons. UE, règl. (UE) n° 910/2014, 23 juill. 2014 : JOUE n° L 257, 28 août 2014, p. 73 ; JCP E 2017, 1005 ; JCP E 2017, 1264*). Pour l'établissement des actes juridiques électroniques, comme pour toute autre facette de l'identification électronique, ce nouveau texte européen a mis au cœur de son dispositif une réglementation technique européenne nourrie des fruits de la normalisation technique, puisque la Commission a reçu le pouvoir d'ériger, par la voie d'actes délégués, ces normes, souples par leur nature propre, en règlements.

2. - L'absorption du règlement e-IDAS par le décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique. - Le nouvel article 1367 du Code civil, issu de l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations (*Ord. n° 2016-131, 10 févr. 2016 : JO 11 févr. 2016, texte n° 26 ; JCP E 2016, act. 151 ; JCP E 2016, 1283*), a maintenu la présomption par le fait d'une souveraineté nationale encore subsistante. Il a aussi maintenu le renvoi à la réglementation française alors en vigueur. La situation est restée en *stand by* un certain temps après l'entrée en vigueur du règlement e-IDAS le 1er juillet 2016, la communication des pouvoirs publics restant pour le moins discrète sur les évolutions en cours. La période de transition devait s'achever en juillet 2017.

Le 28 septembre 2017, le décret conjoint du Premier ministre, de la garde des Sceaux et de la ministre des outre-mer n° 2017-1416 (*D. n° 2017-1416, 28 sept. 2017 : JO 30 sept. 2017, texte n° 8*) a abrogé expressément le décret du 30 mars 2001. Le dispositif de substitution tient dans un seul article, qui lie la présomption du droit français à l'hypothèse d'une signature qualifiée au sens du droit européen : « *La fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée.*

Est une signature électronique qualifiée une signature électronique avancée, conforme à l'article 26 du règlement susvisé et créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement ».

Ce texte met en lumière une sélection des articles du règlement européen. L'article 26 concerne les conditions standard de la fiabilité propres à la signature avancée, qui est une forme embryonnaire seulement de signature qualifiée, dotée de garanties d'authentification du signataire et d'intégrité du contenu de l'acte. Les articles 28 et 29 posent les conditions spécifiques d'une signature qualifiée. L'article 28 impose que l'identification du signataire soit établie via un certificat qualifié répondant à certaines exigences nécessaires et suffisantes, avec un renvoi à l'annexe I du règlement européen. L'article 29 régit quant à lui les exigences relatives aux dispositifs de signature électronique (clé USB, logiciels ou autres), qui sont employés pour lier la signature aux données électroniques constituant l'écrit.

3. - Au-delà de la lettre du décret du 28 septembre 2017. - Le système de la signature sécurisée issu des textes nationaux antérieurs ne se limitait pas, comme on l'a précédemment indiqué, au décret du 30 mars 2001. Les réglementations complémentaires au décret précitées ne sont pas visées par le récent décret, qui n'a au demeurant pas été l'occasion d'une présentation pédagogique du système européen (comp. avec la loi belge du 18 juillet 2017 relative à l'identification électronique, publiée le 9 août 2017).

De son côté, le règlement e-IDAS a, effectivement, créé un dispositif complet qui recouvre le dispositif réglementaire français. Au travers des articles 17 et 18, il dessine le modèle d'organisation qui s'étend peu à peu à la régulation confiée, pour d'autres causes telles que la concurrence ou la protection des données à caractère personnel, à différentes autorités administratives indépendantes : unicité de l'autorité nationale désignée comme organe de contrôle par l'État membre vis-à-vis de l'Union européenne (à quoi s'ajoute une responsabilité personnelle des organismes), obligation de surveillance des pratiques par cette autorité dont l'État membre répond, assistance mutuelle et coopération entre les autorités nationales.

Dès le 24 février 2015 (*JOUE n° L 53, 25 févr. 2015, p. 14*), la Commission européenne a pris une décision relative aux modalités de la coopération entre les États membres en matière d'identification électronique. En France c'est l'Agence Nationale de la Sécurité des Système de l'Information (ANSSI), aujourd'hui rattachée au secrétaire général de la défense et de la sécurité nationale, qui assurera ces fonctions dans la continuité des compétences pour lesquelles elle avait été auparavant créée.

En France, le mécanisme de la présomption attachée aux actes électroniques sécurisés donne un relief particulier à ce cadre réglementaire, car, s'agissant des actes concernés par cette présomption, des certifications doivent impérativement intervenir. Une telle certification fait intervenir, en pratique, des professionnels, que l'on dénomme en pratique « tiers de confiance » et dont la fonction est de contribuer à une mission d'intérêt général, mais par les voies d'une activité à but lucratif. À ce titre, la relation entre le professionnel qui réclame la certification et l'entité qui le contrôle s'inscrit dans l'ordre des relations commerciales. Le règlement e-IDAS comporte des dispositions relatives aux entités chargées de procéder aux évaluations et certifications des tiers de confiance pour certifier les produits et les prestations de délivrance de certificats qualifiés.

L'ANSSI a pris en charge l'élaboration du dispositif de référence national adapté au moyen de documents publiés sur son site Internet, qui revisitent les procédures de certification des tiers de confiance (*Processus de qualification d'un produit, 12 janv. 2017, n° 274/ANSSI/SDE, Ref : QUAL-PROD-PROCESS/1.0 ; Prestataires de services de confiance qualifiés, Critères d'évaluation de la conformité au règlement eIDAS, Version 1.2, 5 juill. 2017*). Ils ont vocation à s'imposer à l'évaluation des certificateurs et émanent, pour autant, d'une agence nationale dont le pouvoir normatif n'est sans doute pas des plus évident. À la différence des autorités administratives indépendantes dont le pouvoir normatif est bien connu, l'ANSSI n'est investie par aucun texte d'un tel pouvoir normatif (en particulier, ce pouvoir n'est pas énoncé dans *D. n° 2009-834, 7 juill. 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », NOR : PRMD0914748D*). L'orthodoxie supposerait que les documents ne soient pas considérés comme ayant une portée contraignante propre, y compris une autorité de fait, ce qui pourrait être justifié par le fait qu'ils aient pour seule vocation d'appliquer le règlement européen. Mais, en réalité, seule une appréciation fine propre à faire comprendre si les documents comportent ou non une part interprétative pourrait aider à trancher.

4. - Les référentiels techniques déclinant les standards posés par le règlement e-IDAS en suspens et l'impossible signature qualifiée à distance. - Le canevas des référentiels techniques nécessaires pour clarifier et harmoniser les différents standards du règlement e-IDAS relatifs aux conditions techniques de sécurisation de la signature qualifiée est encore loin d'être achevé. Les décisions d'exécution de référence les plus précises en termes d'exigences techniques opérationnelles datent des 25 et 26 avril 2016 et concernent les dispositifs de signature (*Comm. UE, déc. d'exécution (UE) 2016/650, 25 avr. 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique : JOUE n° L 109, 26 avr. 2016, p. 40*).

Elles mentionnent certaines normes techniques élaborées au sein du Comité européen de normalisation et ou d'organismes internationaux (ISO et ETSI). Mais, outre le fait que les référentiels techniques sur les *process* de délivrance des certificats qualifiés ne sont, eux, pas précisés par des décisions d'exécution, une restriction de taille affecte la certification des dispositifs de signature :

« *Conformément au considérant 56 du règlement (UE) n° 910/2014, la certification en vertu des articles 30 et 39 dudit règlement ne devrait pas s'étendre au-delà de la protection des données de création de signature électronique, et les applications de création de signature électronique ne sont pas couvertes par la certification* » (*Comm. UE, déc. d'exécution (UE) 2016/650, 25 avr. 2016, préc., consid. 7*).

Il s'en déduit que la réalisation d'un acte accessible à la présomption de preuve littérale via une signature qualifiée reste une hypothèse fragile. Sous réserve que soient, par ailleurs, satisfaites les conditions de l'archivage sur lesquelles le règlement e-IDAS est malheureusement resté muet, la possibilité de dispositifs de signatures sécurisées se dessine néanmoins concernant les actes réalisés dans un environnement maîtrisé par les parties à l'acte, c'est-à-dire en dehors des voies de l'Internet. En revanche, conformément à ce que le règlement e-IDAS avait lui-même clairement annoncé, l'hypothèse d'une signature sécurisée à distance par les voies de l'Internet reste exclue. *A priori*, il n'y a pas de bonne raison d'intérêt général de fustiger cette prudence du règlement européen, qui rejoint la posture française initiale. Même sans le bénéfice de la présomption légale, la signature électronique se porte, en effet, fort bien en droit positif. Quant aux attentes de développement du marché de la certification, la présomption légale attachée à la signature qualifiée n'en est pas pour l'instant le ressort escompté. Mais les voies classiques restent ouvertes, supposant donc, d'une part, une capacité de la part des tiers de confiance à rendre crédible l'intérêt de leurs prestations en vue du développement de la signature avancée et, d'autre part, un cadrage rigoureux des conditions de la labellisation (*Où va la normalisation ? - En quête d'une stratégie de compétitivité respectueuse de l'intérêt général, Rapp. d'information, É. Lamure, n° 627, 2016-2017, 12 juill. 2017*).