25 La signature électronique en pratique : quelle opportunité ?

La signature électronique est devenue essentielle dans le processus contractuel. La notion est cependant source d'incertitudes. Quelle opportunité donc pour la signature électronique ? Le point sur cette question par Alexandre Ghanty, membre de la cellule doctrine de CMS Francis Lefebvre Avocats.

1 A l'heure du tout-numérique, la signature électronique devient un incontournable du processus contractuel. Dernier exemple en date : l'arrêté du 12 avril 2018 relatif à la **signature électronique dans la commande publique**, qui requiert des acheteurs au titre de marchés publics qu'ils se dotent, à compter du 1er octobre 2018, d'une signature électronique avancée basée sur un certificat qualifié.

2 Les **avantages de l'écrit électronique** ne sont en effet pas négligeables. L'archivage s'en trouve facilité ; le processus de contractualisation est simplifié, pouvant permettre d'éviter des paraphes souvent chronophages ; la gestion des documents contractuels l'est également, la formalité du double pouvant alors être réputée satisfaite si le procédé utilisé permet à chaque partie de disposer d'un exemplaire sur support durable ou d'y avoir accès, sous certaines conditions (C. civ., art. 1375 al. 4)… Pourtant, la **notion**-même de signature électronique est source d'**incertitudes** : signatures électronique et manuscrite ont-elles la même valeur dans notre droit ? Comment créer une signature électronique ? Fondamentalement, à quoi correspond la signature électronique ?

Notion de signature électronique

3 Le **droit français** ne nous est pas d'une aide décisive, la notion de signature électronique n'y faisant l'objet d'aucune définition substantielle. L'article 1367 du Code civil expose bien les **conditions** requises pour lui conférer une valeur identique à celle d'une signature manuscrite, mais sans plus de précision quant à sa nature propre : « lorsqu'elle est électronique, [la signature] consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».

Une telle démarche n'est au demeurant pas surprenante : la signature manuscrite ne fait elle-même l'objet d'aucune définition qui permettrait de cerner le champ des pratiques admises à titre de signature. Comme toutes les signatures, la signature électronique doit identifier son auteur et manifester son consentement aux obligations qui découlent de l'acte (C. civ. art. 1367, al. 1). Mais il s'agit là d'exigences applicables à toute opération ou à tout procédé qui se voudrait constitutif d'une signature, et non d'éléments distinctifs de nature à isoler telle ou telle pratique comme signature. **L'absence de définition** laisse ouverte la catégorie des signatures, notamment électroniques, à l'innovation et aux techniques et procédés nouveaux.

4 Le **législateur européen** a pu en proposer une définition dans son règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (Règl. 910/2014 du 23-7-2014, dit « eIDAS »). Cependant, la généralité des termes employés est symptomatique du caractère largement inclusif de la notion : **constituent une signature électronique** 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 » (Règl. eIDAS art. 3, 10). Si elle ne permet pas de déterminer exactement ce à quoi peut correspondre une signature électronique, une telle définition fournit cependant quelques indications.

> *« La signature électronique ne figure pas sur le document signé »*

5 Tout d'abord, la signature électronique correspond à une **suite de données**. Ces données, électroniques, doivent être uniques afin de permettre l'identification du signataire. On perçoit d'emblée les problèmes que cela peut susciter : de prime abord, s'agissant essentiellement de données à caractère personnel, il conviendra de s'assurer que les exigences issues de la réglementation afférente à la protection des données personnelles sont bien respectées. Hormis ces considérations, les techniques et procédés de traitement de telles données devront permettre de caractériser un lien d'imputabilité entre la signature et la personne du signataire.

6 Ensuite, la signature électronique suppose une utilisation de ces données par le signataire via un **processus d'association aux données électroniques à signer**. Toute analogie formelle avec la signature manuscrite doit être à cet égard écartée : la signature électronique n'est pas « apposée » sur un document à signer. Concrètement, la signature électronique **ne figure pas** sur le document signé.

ALEXANDRE GHANTY
Juriste, membre de la cellule doctrine, CMS Francis Lefebvre Avocats

Juriste au sein du cabinet CMS Francis Lefebvre Avocats, A. Ghanty intervient spécifiquement sur les sujets IP/IT/protection des données personnelles. Titulaire du Magistère – DJCE Juriste d'Affaires de l'Université Panthéon-Assas, il rédige actuellement une thèse sur l'investissement en production culturelle.

VISIBILITÉ DE LA SIGNATURE ÉLECTRONIQUE

La signature électronique n'est pas apposée sur le document signé et n'est pas « visible », en tant que telle, sur ce document. Mais certains dispositifs de création de signature permettent l'apparition d'une mention faisant part de l'existence de la signature. Ainsi **par exemple** des reproductions de signatures manuscrites signifiant la présence d'une signature électronique, ou encore des mentions « ce document est signé électroniquement par... », qui ne font que formaliser pour le destinataire du document l'existence d'une signature autrement inintelligible.

La signature électronique est en revanche incorporée au document, les données de signature étant associées aux données résultant du document à signer.

7 Doivent ainsi être a priori exclues du champ des signatures électroniques les **signatures numérisées** puis collées sur les documents à signer : d'une part, elles ne permettent souvent pas une parfaite identification des signataires, sauf à ce que le logiciel utilisé organise un traçage effectif de la personne du signataire (CE 17-7-2013 n° 351931 ; CA Fort-de-France 14-12-2012 n° 12/00311 ; en sens contraire, mais minoritaire, CA Aix-en-Provence 27-4-2017 n° 15/06339) ; d'autre part, elles ne résultent pas d'une réelle association aux données à signer.

8 En tout état de cause, la signature électronique ainsi définie suppose l'utilisation de procédés spécifiques, afin d'assurer en amont une **association correcte des données**, c'est-à-dire une association de nature à empêcher toute altération du document lors du processus de signature, et en aval une **vérification des données** auxquelles les données de signature ont été associées, en vue de savoir si le document a bien été signé et par qui.

La signature électronique en pratique

9 A cet égard, les technologies de la cryptographie sont d'un apport essentiel dans la mise en œuvre de la signature électronique : elles permettent en effet une sécurisation par voie de chiffrement du document signé, en le transformant en une **empreinte numérique** inaltérable sans le consentement du signataire. Concrètement, le procédé de signature électronique le plus classique peut être décomposé en trois phases.

« Le certificat électronique doit permettre une vérification de l'identité du signataire »

10 Dans un premier temps, le **document** à signer est **converti** en une série de chiffres et de lettres : on parle d'empreinte numérique du fichier, produite par un logiciel de hachage. Cette **empreinte** est spécifique au document à signer, et permet donc de déceler toute modification ultérieure éventuelle des données. Par ailleurs, elle ne peut permettre de reconstituer le document d'origine : on dit que la fonction de hachage est une fonction à sens unique, ce qui est de nature à accroître encore la sécurité des données à signer. Cette empreinte est transmise au signataire en même temps que le document à signer. S'ensuit l'opération de signature à proprement parler.

11 Deuxième étape, la **signature** par le signataire. Elle **s'effectue** à l'aide d'un fichier électronique spécifique, un « **certificat électronique** », qui **comprend** d'une part un certain nombre d'informations personnelles le concernant afin d'attester de son identité, et d'autre part une clef algorithmique qui lui est spécifique et qui permettra le chiffrement de l'empreinte numérique, c'est-à-dire sa transformation pour la rendre inintelligible au tiers qui ne disposerait pas de la clef nécessaire pour la décoder.

Ce certificat électronique est **produit** dans le cadre d'un dispositif de création de signature, sur la base des informations personnelles fournies par le signataire de nature à permettre une vérification de son identité. Il **peut se présenter sous diverses formes en pratique** : il peut être enregistré sur clef USB, sur carte à puce, via une application logicielle sur le disque dur du terminal du signataire, ou encore être stocké sur une plateforme à laquelle le signataire pourra accéder en ligne. Le processus de signature consiste alors en l'application de la clef algorithmique de chiffrement à l'empreinte numérique du document : en résulte une empreinte chiffrée, qui ne pourra être décodée que par son destinataire.

12 Dernière étape, l'empreinte ainsi chiffrée est communiquée au **destinataire**, en possession **d'une clef de déchiffrement**, ou « clef publique ». Le destinataire sera ainsi en mesure de vérifier que le document a bien été signé et qu'il n'a pas été altéré, en appliquant sa clef publique à l'empreinte qui lui a été transmise, et en en confrontant le résultat à l'empreinte numérique originelle.

13 Le **procédé** est techniquement séduisant. Son efficacité repose cependant sur un certain nombre de conditions, afférentes à la **sécurité des systèmes**.

LA BLOCKCHAIN COMME SIGNATURE ÉLECTRONIQUE ?

La blockchain constitue une technologie de stockage et de transmission distribuée de transactions, qui fonctionne de pair à pair, en principe sans tiers centralisateur. Chaque bloc de la blockchain regroupe des transactions vérifiées et validées par certains participants du réseau (les « mineurs ») : autrement dit, l'inscription d'une transaction dans la blockchain n'est possible qu'après validation des mineurs par consensus. La sécurité du dispositif est assurée par l'utilisation en pratique des mêmes outils cryptographiques que ceux de la signature électronique.

A cet égard, la blockchain pourrait accueillir le dépôt des empreintes numériques des documents à signer, et ainsi permettre une vérification plus étroite de l'intégrité du document.

Ainsi conçue, elle ne semble toutefois pas de nature à certifier le lien entre la signature et le signataire : aucune vérification de l'identité du participant à la blockchain n'est a priori opérée. Une telle vérification d'identité pourrait certes être mise en place, mais elle conduirait en pratique à une remontée d'informations vers une autorité centrale. L'intérêt du recours à une blockchain, par essence décentralisée, serait alors moindre...

D'une part, les **techniques utilisées** doivent permettre un chiffrement incontournable, « incrackable », de l'empreinte du document à signer, sans quoi l'intégrité des données signées pourrait être remise en cause.
D'autre part, la **délivrance du certificat** et la création de la clef privée au profit du signataire doivent être soumises à des **conditions strictes** de nature à garantir l'authenticité de la signature, c'est-à-dire l'identité du signataire et l'imputabilité de la signature. C'est dans cette perspective que le régime de la signature électronique fait l'objet d'un encadrement strict.

Le régime de la signature électronique

14 Les effets de la signature électronique sont reconnus en droit : ainsi que l'énonce le législateur européen, « une signature électronique ne peut pas être refusée comme preuve en justice au seul motif qu'il s'agit d'une signature électronique ou qu'elle n'est pas qualifiée » (Règl. eIDAS art. 25, 2). Est-ce pour autant à dire que la signature électronique revêt la même **force probante** que la signature manuscrite ? Oui, nous répond l'article 1367 du Code civil, mais à **condition** qu'elle « consiste en un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ». La fiabilité du processus doit être démontrée, à deux niveaux essentiellement : quant à l'identité du signataire tout d'abord, quant au lien entre le signataire et l'acte signé ensuite.

15 La **preuve** de la fiabilité peut être délicate à apporter en pratique. Le législateur la facilite à certains égards : la **fiabilité du processus** sera **présumée** jusqu'à preuve du 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. Le décret 2017-1416 du 28 septembre 2017 précise ces conditions : « 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 », c'est-à-dire « une signature électronique avancée, conforme à l'article 26 du règlement [eIDAS] (voir ci-dessous n° 18) 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 » (voir ci-dessous n° 21).

Est en substance ici reprise la définition de la signature électronique qualifiée au sens du règlement eIDAS.

Qu'est-ce qu'une signature électronique qualifiée ?

16 Le règlement définit trois niveaux de signature : la signature électronique dite simple, la signature avancée et la signature qualifiée, la dernière requérant la caractérisation préalable des deux premières.

« La signature électronique qualifiée est la seule à être présumée fiable »

17 La **signature dite simple** ne revêt aucune spécificité particulière : elle est en quelque sorte le socle commun à toute signature électronique. Ses éléments sont communs à toutes les signatures, y compris les signatures électroniques avancées et qualifiées : quelle que soit la signature utilisée, il s'agira en tout état de cause de données sous forme électronique, jointes ou associées logiquement à d'autres données sous forme électronique, et que le signataire utilise pour signer.

18 Les procédés et techniques utilisés peuvent cependant se conformer à des exigences de sécurité supérieures. En particulier, la signature électronique pourra prétendre à la qualification de **signature avancée** si les conditions suivantes sont remplies :
- la signature est liée de manière univoque au signataire ;
- elle permet d'identifier le signataire ;
- elle est liée aux données associées à cette signature, de telle sorte que toute modification ultérieure soit détectable ;
- elle a été créée à l'aide de données de création de signature que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif.

19 Les **conditions de qualification** de la signature avancée reprennent en substance les éléments essentiels de la signature électronique tels que mis en exergue par le règlement, mais en précisent les exigences en termes de sécurité. Il ne suffit plus que la signature électronique résulte de données utilisées à cette fin par le signataire, encore faut-il que ces données et la signature créée permettent d'identifier le signataire de manière univoque. Il ne suffit plus non plus que les données de signature soient associées aux données de l'acte à signer, encore faut-il que cette association permette la création d'un lien d'inaltérabilité entre la signature et l'acte en question, ou du moins rende détectable toute altération de l'acte signé.

20 Précision intéressante : le signataire peut désormais créer sa signature électronique à l'aide de données de création qu'il utilise sous son **contrôle exclusif**. Nous noterons à cet égard l'évolution rédactionnelle : il n'est plus nécessaire que la signature soit créée à l'aide de données dont le signataire détiendrait le contrôle, par exemple sur une **clef** USB qui serait **remise physiquement** au signataire, ainsi que le requérait l'ancien décret 2001-272 du 30 mars 2001 portant transposition de la directive 1999/93 du 13 décembre 1999.
Le règlement eIDAS fait preuve de plus de souplesse à cet égard : il est désormais possible que les données de création soient détenues sur une **plateforme de service à distance**, sous réserve toutefois que soit assuré un niveau de confiance élevé pour le signataire dans l'utilisation des données de création. En pratique, la clef privée générée au bénéfice du signataire pourra donc être activée à distance par le signataire auprès de la plateforme hébergeuse, à condition toutefois que soit mis en place un **dispositif d'authentification du signataire** avec vérification de son identité, par exemple par le biais d'un code d'activation envoyé au signataire par SMS ou par courrier électronique.

21 La **signature dite qualifiée** porte à un degré encore supérieur ces exigences. En substance, elle constitue une signature avancée, mais doit se conformer au surplus à des **exigences de sécurité additionnelles** : d'une part, la signature doit être créée à l'aide d'un dispositif de création de signature qualifié ; d'autre part, elle doit reposer sur un certificat qualifié de signature électronique. **Concrètement**, la signature qualifiée est une signature avancée qui a passé l'épreuve de la qualification. Cette qualification est double : elle concerne tant le dispositif de création de la signature que le certificat délivré au signataire.

22 Pour être qualifié, le **dispositif de création de signature** doit répondre aux exigences de l'article 29 du règlement

eIDAS, lequel renvoie à la liste de son annexe II. Ces exigences visent à assurer la fiabilité et la protection du dispositif de création, essentielles dans une perspective de sécurité des données personnelles recueillies auprès du signataire, mais surtout afin de garantir l'imputabilité de la signature et son authenticité. La qualification du dispositif de création de signature se **matérialise** en pratique par une **certification de l'Agence nationale de la sécurité des systèmes de l'information** (ANSSI). Cette certification différera selon que les données de création de la signature restent ou non sous le contrôle total du signataire : le dispositif de création devra ainsi faire l'objet d'une certification supplémentaire des systèmes ou produits concourant à protéger la clef privée contre une utilisation par d'autres que le signataire si les données ne sont pas détenues par le signataire. Le risque de faille et d'utilisation indue du dispositif de signature est en effet accru dans une telle hypothèse.

23 De manière similaire, la **qualification du certificat de signature** est **subordonnée** au respect d'un certain nombre d'exigences résultant de l'annexe I au règlement, sur renvoi de l'article 28. Le certificat, produit sur la base des données du signataire et qui permet de générer la clef privée utilisée pour signer, doit en effet être émis dans des conditions de nature à en garantir l'authenticité. La **conformité des certificats qualifiés aux normes eIDAS** est évaluée par l'ANSSI en France. Par ailleurs, le certificat qualifié doit être émis par un **prestataire de services de confiance** lui-même qualifié par l'ANSSI en France.

24 Les **conditions de remise du certificat** sont essentielles en vue de garantir l'imputabilité de la signature. Intuitivement, la solution la plus sécurisante résiderait dans la remise **en main propre** du certificat au signataire : elle permet en effet une vérification immédiate de l'identité du destinataire, par exemple sur présentation à l'agent d'une pièce d'identité comprenant photographie et données d'identification. C'est notamment l'option retenue dans le cadre des **téléprocédures administratives**, qui requièrent un contrôle en face à face du client : la personne physique doit alors présenter un document officiel d'identité avec photographie qui sera vérifié par le personnel du prestataire en question.

COMMENT IDENTIFIER LES « PRESTATAIRES DE SERVICE DE CONFIANCE QUALIFIÉS » ?

L'ANSSI publie régulièrement une liste de confiance, comprenant des informations relatives aux prestataires et aux services qu'ils fournissent, isolant notamment les prestataires de services de confiance qualifiés et leur service de délivrance de certificats qualifiés.
L'identification d'un certificat qualifié en France passera donc en pratique par l'examen de cette liste de confiance régulièrement publiée par l'ANSSI.
Une telle identification peut s'avérer plus délicate s'agissant de **prestataires situés au sein d'autres Etats membres** de l'Union européenne. Nous noterons cependant que la Commission européenne met à la disposition du public un outil permettant de parcourir les listes de confiance nationales (https://webgate.ec.europa.eu/tl-browser/#/).

« Le certificat électronique peut être remis en main propre ou délivré à distance »

Cependant, le règlement admet également que le certificat puisse être délivré **à distance** (art. 24) : la remise devra alors s'opérer sur vérification d'un « moyen d'identification électronique pour lequel, avant la délivrance du certificat qualifié, la personne s'est présentée en personne, et qui satisfait aux exigences des niveaux de garantie substantiel ou élevé ». En pratique, le prestataire concerné ne pourra accepter que trois **types de moyens d'identification électroniques**, à savoir : ceux ayant fait l'objet d'une notification par l'un des Etats membres ; ceux présentant un niveau de garantie substantiel ou élevé, c'est-à-dire permettant une réduction substantielle voire éliminant tout risque d'utilisation abusive ou d'altération de l'identité du signataire ; ou encore ceux pour lesquels a été publiée une documentation permettant d'établir, sans ambiguïté, que la présence physique du demandeur est un prérequis à l'obtention de ce moyen d'identification.

En conclusion : oui à la signature électronique, à condition qu'elle soit qualifiée

25 Ses effets juridiques étant alignés sur ceux de la signature manuscrite, la signature électronique présente un grand nombre d'avantages, ne serait-ce qu'en termes d'optimisation des processus contractuels et de réduction des coûts qu'elle peut impliquer. Encore faut-il être en mesure de pouvoir démontrer la fiabilité du processus de signature, ce qui peut constituer une tâche ardue au regard de la technicité et de la complexité des procédés en présence. Une **pratique raisonnable et sécurisante** pour les parties semble résider dans le recours aux seuls dispositifs de signatures qualifiées. Aisément identifiables du fait des certifications et qualifications ANSSI qu'ils requièrent en pratique, de tels dispositifs présentent l'avantage de présumer une telle fiabilité.