
Signature électronique

Etat des lieux et perspectives



MONIA GRUBER

DÉCEMBRE 2020





Depuis la généralisation des outils informatiques comme interface entre les consommateurs et les entreprises à la fin des années 90, et la recherche, tirée en avant par les entreprises digitales telles que les GAFAM, de toujours plus de digitalisation dans les échanges commerciaux, des formes diverses de vérification d'identité et de formalisation des engagements contractuels ont vu le jour, supportées – mais souvent suivies – par la législation, qui en a validé progressivement, depuis le début des années 2000, la valeur d'engagement moral, puis la valeur juridique d'opposabilité[1].

Ces formes de signature ont ouvert la voie, d'une part, à une digitalisation plus grande des interactions contractuelles, mais également, et on l'a vu avec la crise qui a secoué l'année 2020, à une interaction complètement à distance dans les cas où celle-ci est préférable.

On trouve aujourd'hui différentes formes de signatures digitales et électroniques. Si la signature digitale impose au signataire d'être présent pour pouvoir apposer physiquement sa signature sur une tablette à l'aide d'un stylet, la signature électronique peut, elle, être réalisée en ligne et à distance. Grâce à cette évolution technologique, de nombreuses opérations – telle que la signature d'une souscription à une offre bancaire – sont alors simplifiées. Les entreprises peuvent dès lors proposer un parcours totalement digital à leurs clients.

Pour certains, cette forme de signature représente une révolution technologique permettant de gagner du temps, en évitant de fastidieuses prises de rendez-vous dans des agendas débordés, mais pour d'autres, il s'agit d'un système incompréhensible et déshumanisé, auquel il est difficile d'accorder sa confiance.

Mais qu'est-ce, précisément, que la signature électronique, aussi appelée "signature à distance" ?

Il s'agit d'un procédé informatique permettant d'effectuer une identification formelle du signataire, en assurant de fait l'identité de la personne ayant envoyé et signé le document digital, tout en garantissant la non-altération du document entre la consultation et le moment de la signature. Entre rapidité et simplicité, la gestion de tout type de contrat peut se faire en quelques clics et à travers toute l'Europe.

Nous allons détailler, dans la suite de cet article, les formes que peut prendre la signature électronique.

[1] la directive 1999/93/CE sur le droit de la preuve en concernant la signature électronique et l'acte authentique électronique.



4 types de signature électronique

Rentrons plus en détail dans les mécanismes propres à la signature électronique. Elle se décline sous quatre formes : simple, avancée, avancée avec certificat qualifié, qualifiée. Chacune a différents niveaux de prérequis, entraînant différents niveaux de protection, en fonction du besoin de l'utilisateur.

- **la signature électronique simple**

Comme son nom le sous-entend, c'est la version la plus accessible des signatures électroniques. Elle est rapide à installer pour l'entreprise, et facile à utiliser pour le signataire. Elle requiert un système appelé « authentification à double facteur », processus permettant au client de valider sa signature à distance en recevant, par exemple, un SMS contenant un mot de passe à usage unique (également appelé One Time Password - OTP) qui devra ensuite être reporté sur la plateforme de signature à distance. Cette opération n'est cependant réalisable que si le signataire possède le matériel technologique requis, ainsi qu'une connexion réseau lui permettant d'accéder au service. Si ces conditions ne sont pas respectées, alors la signature électronique à distance simple ne pourra être utilisée. Ce type de signature est utilisé, par exemple, pour signer un contrat de travail ou des accords de confidentialités entre entreprises.

Mais qui dit signature électronique simple, dit processus simplifié. Et de fait, il n'y a aucune exigence de sécurité établie, si ce n'est l'utilisation du mot de passe à usage unique, qui permet de renforcer le processus en y ajoutant une étape de validation, démontrant que le signataire est bien en possession du téléphone de la personne qu'il dit être, offrant un certain niveau de confiance – somme toute limité – dans son identité.

Bien qu'un dossier de preuve (faisceau de preuves techniques prouvant que le signataire a procédé à la signature du document à distance, par exemple via reconnaissance de son numéro de portable et le moment exact de la signature – date et heure) ne soit pas indispensable, il est fortement conseillé en cas de contestation. Notons que dans ce type de signature électronique, l'absence d'un sceau certifiant la non-altération et non modification du document rend impossible de prouver l'authenticité du document. Ceci nous amène au principal inconvénient de ce mode de signature : le manque de sécurité totale et de preuve en cas de litige. Cette signature séduit par la facilité avec laquelle elle peut être mise en œuvre et utilisée au quotidien pour des transactions simples, mais son niveau de sécurité requiert un certain niveau de confiance entre les parties, et présente donc un réel désavantage pour toute entreprise souhaitant établir un dossier de solide à l'appui de la validité des engagements signés...

- **la signature électronique avancée**

Les faiblesses de la signature électronique simple ont amené au développement d'un deuxième type de signature : la signature électronique avancée. Prenons l'exemple des établissements bancaires en Europe. Grâce à la signature électronique avancée, toute personne peut ouvrir un compte bancaire dans une agence dans n'importe quel pays européen, sans même avoir besoin de s'y rendre physiquement, en utilisant un « token d'identification[2] » reçu à domicile, qui permet de garantir son identité en ligne et en toute sécurité (tant que le token n'est pas dérobé !). A la différence de la signature électronique simple, la signature électronique avancée possède des systèmes de vérifications plus précis, et un niveau de sécurité plus élevé, tels qu'énoncés dans le Règlement Européen eIDAS[3]:

[2] Un token d'identification est un code de 6 caractères nécessaire pour associer vos données d'identité à une ID numérique.

[3] Le règlement eIDAS concerne principalement les organismes du secteur public et les prestataires de services de confiance établis sur le territoire de l'Union européenne. Il instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique. Il couvre notamment le sujet de la signature électronique, et abroge la directive 1999/93/CE. L'ANSSI est l'un des organismes nationaux chargés de la mise en œuvre de ce règlement.



- Respect des normes de signature ETSI[4] et eIDAS sur l'identification électronique et les services de confiance pour les transactions numériques au sein du marché intérieur de l'U.E.
- Usage d'un certificat numérique associé au signataire
- Système poussé de vérification de l'identité du signataire
- Possibilité de prouver que le document n'a pas été modifié depuis la signature

La validité de la signature électronique avancée est renforcée par l'ensemble des systèmes de vérification d'identité déployés lors de l'attribution du « token », et la preuve que le signataire a donné son accord au moment de la signature. Bien que l'installation de ce type de signature soit plus laborieuse et coûteuse sur le court terme, il offre aux entreprises une certaine sérénité et assurance en cas de contestation, et est pleinement en ligne avec les normes de signature ETSI et le règlement eIDAS.

- **la signature électronique avancée avec certificat qualifié**

Allons encore plus loin avec la signature électronique avancée avec certificat qualifié. Ce troisième type de signature électronique possède les mêmes caractéristiques que la signature électronique avancée. S'y ajoute un niveau de sécurité supplémentaire avec une rencontre en face à face permettant le contrôle avancé de l'identité du client. Par exemple, un établissement bancaire pourrait vous demander de venir chercher le token d'identification en personne en agence. Le personnel bancaire peut alors contrôler votre pièce d'identité au moment de la délivrance. Ce type de signature peut engendrer une frustration pour le client dans le cas d'une souscription via un parcours totalement digital, puisque ce dernier ne comprendra pas la nécessité de se rendre en agence alors qu'il a pris le temps de tout faire en ligne au préalable.

Le bémol des deux précédents types de signature est qu'ils requièrent tous deux un investissement digital important de la part des entreprises, notamment pour la mise en place de systèmes d'archivage sécurisés. En revanche, pour une mise en place efficace et une minimisation des coûts inutiles, les entreprises ont tout intérêt à se faire accompagner par des professionnels compétents dans le domaine. Notamment pour mettre en place les niveaux de sécurité au sein de l'entreprise, nécessaires pour se protéger, par exemple, contre le piratage dont pourrait résulter la suppression, la perte, le vol ou l'altération de tout ou partie des données. En effet, l'utilisation des nouvelles technologies ne se fait pas sans risque et requiert une attention particulière à la protection des documents et des données clients détenus. Notons que le risque lié par exemple à la perte ou l'altération de la donnée peut exister tant du côté de l'entreprise que du côté du client, chaque partie peut être exposée à un piratage de ses dossiers.

- **la signature électronique qualifiée**

C'est pourquoi il serait peut-être plus stratégique de se tourner directement vers une signature électronique qualifiée. Elle possède le niveau le plus poussé de sécurité, de quoi rassurer les entreprises et utilisateurs les plus inquiets ! C'est la raison pour laquelle elle est utilisée lorsque l'authenticité de l'acte qu'elle atteste est critique, comme par exemple les actes devant notaire, les exploits d'huissiers de justice, les documents établis par les avocats, les actes produisant des effets dans l'Union Européenne et les actes rédigés auprès d'organismes publics pour lesquels les niveaux de confiance et de sécurités exigés sont très élevés.

[4] L'Institut Européen des Normes de Télécommunications (European Telecommunications Standards Institute).



Dans le cadre de la signature électronique qualifiée, la vérification de l'identité du signataire doit impérativement être faite en personne. A la différence des types de signature précédents, et ce qui représente un réel avantage pour l'entreprise, face à une contestation auprès d'un tribunal, la charge de la preuve s'inverse, c'est-à-dire que le signataire devra prouver qu'il a ou elle n'a pas signé le document, ce ne sera pas à l'entreprise de le démontrer. De fait, la signature est présumée fiable si elle fait appel à un certificat électronique qualifié, ce dernier est délivré par une autorité de certification contrôlé par l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI[5]). Il est vrai que l'environnement juridique de la signature électronique est compliqué, et que les bons interlocuteurs doivent être sollicités pour que l'entreprise s'assure que tous les moyens sont mis en œuvre pour sa sécurité.

Ce type de signature électronique peut séduire les plus réticents en alliant sécurité et confiance. Un autre avantage à garder à l'esprit est qu'elle permet de garder un lien avec le client ... ! A l'heure de la digitalisation des processus, la relation client peut être dégradée et dans certains cas devenir inexistante, déshumanisée par l'utilisation des nouvelles technologies, c'est pourquoi une rencontre lors de la souscription peut être l'occasion de créer un lien spécial qui ne s'oubliera pas, et qui permettra de maintenir les emplois en agence !

Un outil pour faciliter les échanges européens

La signature électronique s'inscrit parfaitement dans un contexte européen d'ouverture économique et de simplification des échanges numériques. En effet, grâce au Règlement Européen eIDAS, un cadre d'interopérabilité est facilité entre les États membres de l'Union Européenne. L'objectif de cette démarche est « de promouvoir le développement d'un marché de la confiance numérique », comme l'évoque l'ANSSI. Le Règlement eIDAS accorde une dimension juridique aux documents traités lors du processus de signature à distance et prévoit des exigences pour « les services de confiance relatifs à la signature électronique, au cachet électronique, à l'horodatage électronique, à l'envoi recommandé électronique et à l'authentification de sites internet » comme l'explique l'ANSSI. Dans le cadre d'opérations et d'échanges intra-européens, les entreprises peuvent alors bénéficier des avantages d'un des quatre processus de signature électronique, le niveau de sécurité sera défini en fonction de leur utilisation et de leurs besoins.

Dans une Europe fortement exposée à la digitalisation, les consommateurs passent une grande partie de leur temps sur leurs smartphones ou tablettes, et la tendance est à la hausse, notamment avec l'arrivée prochaine de la 5G et les progrès dans le domaine de l'Intelligence Artificielle. La digitalisation des processus client, et plus largement de tous les actes à caractère transfrontalier ayant valeur juridique, est la clé du succès et de la pérennité des entreprises, car elle leur permet de rester compétitives sur un marché toujours plus en proie au digital.

Prenons pour exemple le secteur bancaire. L'essor et le gain rapide de parts de marché des néo-banques peut causer du tort aux établissements plus classiques ne proposant pas ou peu de solution à distance. Notons que selon l'agence d'étude de la performance digitale D-Rating, en 2019, en France, les néo-banques ont dépassé les banques dites « de première génération » en nombre de clients individuels. Fin 2019, 6.1 millions de clients – soit +43% par rapport à 2018 – étaient comptabilisés et partagés entre 11 néo-banques européennes, contre 5.5 millions – soit +15% par rapport à 2018 – pour les 7 banques classiques analysées. Que ce soit à niveau européen ou national, de plus en plus d'entreprises optent pour la signature électronique dans le cadre de la digitalisation de leurs processus. Ayant acquis une certaine compréhension de ces nouveaux processus et de leurs avantages, nombreux sont ceux qui se lancent dans une aventure technologique avec des parcours partiellement ou totalement digitaux.

[5] En France et au Luxembourg, l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI), en Allemagne le Bundesamt für Sicherheit in der Informationstechnik (BSI) et la Melani en Suisse.



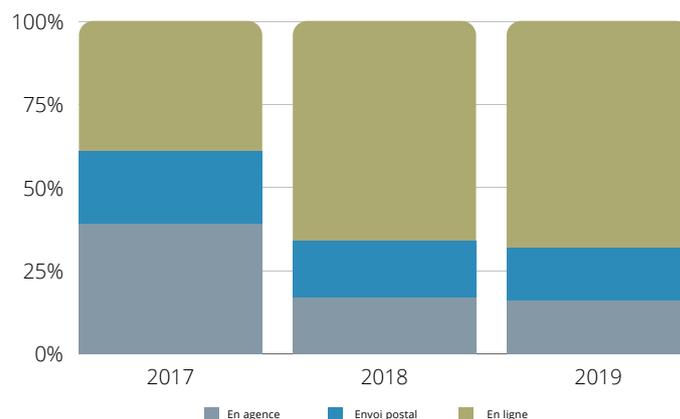
Dans le secteur bancaire toujours, comme mentionné précédemment, pour faire face aux nouveaux acteurs économiques du secteur et rester compétitifs face aux Fintechs, l'ouverture d'un compte ou la souscription à un nouveau service peuvent maintenant être faites presque exclusivement à distance dans la majorité des grands groupes. Selon une étude menée par D-Rating, en 2019, 68% des banques de détail proposaient d'ouvrir un compte en banque totalement à distance, soit 30 pourcents en plus en comparaison avec 2017. Les néo-banques profitent elles aussi des avantages de la signature et l'identification client à distance – via vidéoconférence notamment – puisqu'elles offrent la possibilité aux clients de souscrire à une offre bancaire intégralement en ligne.

Pour le secteur de l'assurance non-vie (IARD), la souscription d'une offre de couverture peut aussi être faite à distance grâce à la signature électronique. Cette solution est disponible auprès de bon nombre d'assureurs européens, dont les campagnes de dématérialisation d'envergures ont commencé dès 2016. Les compagnies d'assurance misent clairement sur cet outil digital qui permet d'apporter une fluidité aux processus et un gain d'efficacité au sein des entreprises, et en font une publicité de plus en plus active pour tenter de renouer le dialogue avec leurs clients.

En revanche, pour l'assurance vie, nous pouvons constater qu'au Luxembourg notamment, cette révolution technologique n'en est encore qu'à ses balbutiements. Nous pouvons supposer que cela est dû aux enjeux plus élevés en termes de contrats d'assurance vie en comparaison avec les contrats d'assurance IARD, et un besoin client de rencontrer son conseiller pour aborder les différents sujets liés à la souscription d'un contrat d'assurance vie.

Mode de signature des contrats lors de la souscription d'un compte courant

Source : D-Rating 2019



“

Les signatures électroniques représentent un énorme progrès technologique et devraient être adoptées dans de nombreux autres cas d'utilisation et secteurs.

De nombreuses entreprises doivent s'éloigner de leur opinion selon laquelle les signatures électroniques coûtent beaucoup d'argent. Les avantages qualitatifs et quantitatifs de la mise en œuvre des processus de signature électronique dépassent largement les coûts. En outre, le prix unitaire payé pour les signatures électroniques est bien inférieur à ce qu'il en coûte aux entreprises pour s'en tenir aux flux de travail à l'ancienne et à la paperasse interminable.

Si l'on considère le taux d'adoption actuel des signatures électroniques dans le monde et en particulier dans les régions technologiquement avancées, comme l'Europe occidentale ou la Scandinavie par exemple, les signatures électroniques sont déjà proches d'une norme plutôt que d'une exception. Ce n'est qu'une question de temps avant que même les secteurs les plus traditionnels adoptent cette puissante technologie.

Felix Hemmerling, co-founder & CEO at kodehyve

”



Perspectives pour le futur

L'année 2020 a été marquée par la pandémie de COVID-19 et ses tragiques conséquences en Europe, comme partout dans le monde. Dans un contexte où les individus sont invités à limiter leurs interactions physiques, la digitalisation des processus se présente encore plus que par le passé comme une solution incontournable. Elle permet de limiter les déplacements puisque tous les documents peuvent dorénavant être signés depuis chez soi. C'est une solution incontournable qui permet aux entreprises de poursuivre leur activité à distance tout en protégeant leur clientèle des risques liés à cette pandémie dans le cadre d'un déplacement en agence, par exemple. Cette solution requiert toutefois que l'entreprise ait anticipé l'envoi de ses tokens aux clients ! Les entreprises doivent également être conscientes des risques et limites de ces outils technologiques et, en conséquence, mettre en œuvre les actions nécessaires à leur bon déploiement et anticipation.

Cependant, nous ne pouvons pas ignorer les personnes ayant un accès limité ou inexistant aux nouvelles technologies, et qui de fait ne pourront pas bénéficier des avantages de cette solution. La signature électronique reste finalement une possibilité limitée aux utilisateurs ayant les moyens techniques et une compréhension suffisante des nouvelles technologies pour pouvoir s'en servir. C'est aussi un aspect de la mise en place de ce type de technologie que les entreprises ne peuvent ignorer : l'accompagnement de leurs clients dans le changement et la formation à l'utilisation des solutions digitales. Or ces deux aspects sont trop souvent mis de côté, pour des raisons de praticité ou de prix.

Outre ses avantages majeurs, la signature électronique offre bon nombre d'améliorations pour les clients et les entreprises. Les coûts liés à la préparation et l'acheminement des documents sont réduits, l'environnement est respecté dans une certaine mesure (moins de papier, moins de déplacements...), et ce bien que nous ne puissions ignorer le coût environnemental lié aux serveurs informatiques. Dans un monde où tout va très vite et chaque minute est précieuse, les temps de traitement sont nettement réduits, ce qui conduit à une disponibilité plus importante des équipes pour assister les clients, et donc à une gestion plus qualitative et plus efficiente des dossiers. Et dans les cas où le processus fonctionne sans embuche (!) nous pouvons aussi noter une réduction du stress du côté du client qui verra sa demande traitée plus rapidement. De plus, les systèmes de signature à distance possèdent une ergonomie adaptée aux ordinateurs, tablettes et téléphones portables, de quoi séduire un large panel d'utilisateurs. L'expérience client en est améliorée. L'archivage est sécurisé et durable et les documents sont protégés ce qui induit une diminution notable du risque de duplication, de perte ou d'altération.

Cependant, l'inverse est aussi vrai, lorsque le processus est laborieux, le client sera découragé et ne terminera pas ou reportera l'opération qu'il souhaitait effectuer, alors que face à un agent l'accompagnant pas à pas, il serait allé au bout de sa démarche. Dans certains cas, cela peut se traduire par la perte d'opportunités commerciales, et peut avoir des répercussions sur l'activité de l'entreprise. C'est pourquoi, encore une fois, il est important de choisir le type de signature à distance adéquate, c'est-à-dire celui qui maximise le rapport entre niveau de sécurité requis et lourdeur/complexité pour le client. Et il est fondamental pour les entreprises de demander un accompagnement personnalisé, en cas de doute ou d'incertitude quant au choix de la technologie adéquate.

De la signature électronique simple à la signature électronique qualifiée, le spectre des possibles est large pour séduire et convaincre les entreprises dans la construction de leur parcours digital. Bien que cela représente un processus complexe et souvent coûteux à mettre en œuvre, les avantages liés à l'implémentation de la signature électronique, combinés à l'incontournabilité face à la concurrence en ligne, vont certainement convaincre dans un futur proche de nombreuses entreprises qui n'ont pas encore sauté le pas. La récente crise sanitaire, et ses conséquences en matière d'évolution de la relation client, finira de convaincre les plus réticents. Gardons à l'esprit que toute solution technologique présente ses limites et risques, il est alors important pour les entreprises de bien définir leur projet digital et d'anticiper autant que possible les « mauvaises surprises ».

GENÈVE

8, rue du Conseil Général
1205 Genève, Suisse
☎ +41 22 322 13 52
philippe.perles@noveoconseil.com

LUXEMBOURG

26 boulevard Royal
2449 Luxembourg
☎ +352 22 99 99 2417
geoffroy.gailly@noveoconseil.com

PARIS

13 rue Lafayette
75009 Paris, France
☎ +33 1 72 89 72 54
olivier.laloum@noveoconseil.com



MONIA GRUBER

DECEMBRE 2020