Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

Le réseau Lexing vous informe – The Lexing® network informs you

JTIT Internationale n°14 – mars 2017
JTIT Special international issue #14 – March 2017

LA SIGNATURE ÉLECTRONIQUE

ELECTRONIC SIGNATURE

UN OUTIL INDISPENSABLE A LA TRANSFORMATION NUMERIQUE

▪ Aujourd'hui, tout est dématérialisé ou dématérialisable, et la transformation numérique est une tendance irréversible. Dans ce contexte, la signature électronique contribue à instaurer un climat de confiance, essentiel dans l'environnement en ligne, aussi bien pour les consommateurs, les entreprises et les administrations, car elle permet de garantir l'authenticité et l'intégrité des données, ainsi que l'identité du signataire.

▪ La signature électronique soulève de multiples questions (Est-elle équivalente à une signature manuscrite ? Pourquoi, quand et comment l'utiliser ? A-t-elle une valeur légale ? Est-elle vraiment sécurisée ?). Elle peut, en outre, être associée à d'autres services de confiance en ligne, comme le coffre-fort numérique.

▪ Sur le continent européen, le statut juridique de la signature électronique est encadré par le règlement 910/2014 dit « eIDAS ». Dans d'autres pays du monde, des solutions ont également été mises en place par le législateur afin d'accroître l'efficacité et la sécurité de ce service électronique.

Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde. Les pays suivants ont contribué à ce numéro : Afrique du Sud, Allemagne, Belgique, France, Grèce.

A KEY TOOL FOR DIGITAL TRANSFORMATION

▪ *Today, everything is or can be paperless, and digital transformation is an irreversible trend. In this context, electronic signatures contributes to building trust in the online environment, which is essential for consumers, businesses and administrations, as it ensures the authenticity and integrity of the data, as well as the identity of the signatory.*

▪ *The electronic signature raises many questions (Is it equivalent to a handwritten signature? Why, when and how to use it? Has it a legal value? Is it really secure?). It can also be combined with other online trust services, such as the digital safe.*

▪ *On the European continent, the legal status of the electronic signature is governed by the so-called "eIDAS" regulation 910/2014. In other countries of the world, solutions have also been put in place by the legislator to increase the efficiency of electronic services.*

The Lexing® network members provide a snapshot of the current state of play worldwide. The following countries have contributed to this issue: South Africa, Germany, Belgium, France, Greece.

A propos de Lexing®

Lexing® est le premier réseau international d'avocats en droit du numérique et des technologies avancées.
Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leur pays respectifs.

About Lexing®

Lexing® is the first international attorneys' network for digital and advanced technology law.
Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

POLYANNA BIGLE

Tour d'horizon de la signature électronique en Afrique du Sud

▪ En Afrique du Sud, la signature électronique est parvenue à maturité et ceux qui se sont déjà engagés dans cette transition numérique ont pu en mesurer les avantages en termes d'efficacité et de fiabilité. Si les prestataires internationaux de solutions de signature électronique sont bien entendu présents dans le pays, les entreprises locales sont également de la partie et proposent des options innovantes adaptées au contexte africain.

▪ La signature électronique est légale en Afrique du Sud depuis plus de dix ans. Le régime d'accréditation des fournisseurs de signature électronique avancée instauré en 2012 connait un regain d'intérêt et la jurisprudence s'est prononcée sur la législation pertinente pour la première fois en 2014.

▪ Dans un pays en développement en proie à la corruption, miné par une mauvaise qualité des prestations de services et souffrant d'une image négative sur la scène internationale, la signature électronique a l'avantage d'apporter une sécurité juridique.

▪ Les signatures manuscrites sont perçues comme garantissant cette sécurité. Or, cette impression est trompeuse car les signatures manuscrites sont, en fait, peu fiables, faciles à falsifier et souvent sujettes à contestation. En cas de confit relatif à l'authenticité de ce type de signature, le recours à des experts en graphologie est en effet généralement peu efficace, chacune des parties désignant son propre expert afin de contester les conclusions de l'autre. En outre, il peut être difficile de trouver des personnes susceptibles de témoigner de la véracité de cette signature car elles peuvent avoir quitté l'entreprise concernée, être décédées ou tout simplement injoignables.

▪ En revanche, avec une signature électronique, des nombreuses autres méthodes, bien meilleures, permettent de s'assurer de l'identité des signataires et de la nature de leur intention : la vérification par courrier électronique, l'authentification à deux facteurs, ou encore le chiffrement avec infrastructure à clés publiques (ICP). Les méthodes modernes d'authentification associées aux signatures électroniques sont ainsi très efficaces et offrent moins de prises à contestation. De fait, les garanties offertes par la signature électronique sont de loin supérieures à celles de la signature manuscrite.

Cadre juridique

▪ Le cadre juridique sud-africain régissant la signature électronique, tous types de transaction confondus, est constitué par :

- la common law d'Afrique du Sud (issue du droit romano-hollandais et des décisions judiciaires antérieures) ;
- la loi de 2002 sur les communications et les transactions électroniques, dite loi « ECT » **(1)** ; et
- la législation sectorielle.

(1) http://www.gov.za/sites/www.gov.za/files/a25-02.pdf

Common Law

▪ Les tribunaux sud-africains interprètent le terme « signature » selon la définition qui lui est ordinairement donnée dans les dictionnaires, c'est-à-dire le nom d'une personne écrit de sa propre main en vue d'authentifier un document ou un écrit.

▪ Plusieurs éléments clés ressortent de cette définition :

- la signature est le **nom ou** de la **marque** du signataire ;
- le signataire doit l'avoir **apposée lui-même** ;
- et il doit avoir eu **l'intention** qu'elle l'**authentifie**.

▪ Toute signature qui satisfait à ces critères est donc une signature au sens de la common law. La common law applicable aux signatures englobe les signatures électroniques, le législateur ne les ayant pas explicitement exclues de son champ d'application.

Approche fonctionnelle

▪ Pour apprécier si un élément constitue ou non une signature, les tribunaux ont tendance à axer leur analyse sur le critère de l'intention des parties. Autrement dit, si les parties ont souhaité de faire d'un élément leur signature, cet élément sera généralement considéré comme une signature en vertu de la common law.

▪ En outre, d'après la jurisprudence, une signature ne doit pas nécessairement être manuscrite. Une signature électronique sera donc considérée suffisante dès lors que le critère de l'intention des parties est rempli.

▪ Par conséquent, une signature électronique est bien une « signature » au sens de la common law car :

- elle contient le **nom** du signataire (ou toute autre donnée d'identification) ;
- le signataire **l'appose lui-même** en choisissant de l'apposer sur un document ; et
- le signataire **a l'intention** que cette signature l'**authentifie**.

Jurisprudence

▪ Cette approche fonctionnelle a été confirmée par la décision Spring Forest Trading c/ Wilberry de la Cour suprême d'Afrique du Sud **(2)**.

▪ En l'espèce, deux sociétés avaient décidé, par échange de courriels signés électroniquement, de mettre fin au contrat qui les liait. L'une des parties a ensuite contesté en justice la fin de leur relation contractuelle, en invoquant une clause du contrat selon laquelle toute modification de ses dispositions devait être effectuée par un **écrit signé** des parties. Il était donc demandé aux juges de décider si ces courriels signés électroniquement constituaient un écrit signé.

▪ S'agissant de l'exigence d'un écrit, la loi ECT précise qu'un document est écrit si « le document […] se présente [...] sous la forme d'un message de données », étant précisé qu'un contrat « n'est pas dépourvu de force et d'effet juridiques au seul motif qu'il a été conclu [...] au moyen de messages de données ». Dans la mesure où un courriel est une forme de message de données, la haute juridiction a relevé que l'exigence d'un écrit était satisfaite.

▪ S'agissant de l'exigence d'une signature, toujours selon la loi ECT, une signature électronique comprend « les données jointes [...] ou logiquement associées à d'autres données et destinées à servir de signature ». Les juges ont estimé que les noms dactylographiés se trouvant en fin des courriels échangés satisfaisaient à l'exigence de signature énoncée dans le contrat, car ces noms servaient à authentifier l'identité des parties participant à cet échange.

▪ Constatant que les deux exigences posées par le contrat étaient remplies, le tribunal en a conclu que les courriels échangés par les parties pouvaient effectivement entraîner une modification valable du contrat, et que ce dernier avait donc bien été résilié par ce moyen **(3)**.

(2) http://www.saflii.org/za/cases/ZASCA/2014/178.html

(3) « Spring Forest Trading v Wilberry, Michalsons», https://www.michalsons.com/blog/spring-forest-trading-v-wilberry/14861

La loi sur les communications et les transactions électroniques

▪ La position adoptée par la common law est confirmée par la loi ECT **(4)**. Cette loi, qui réglemente de nombreuses communications et transactions électroniques, consacre la validité des signatures sous forme électronique.

(4) "Guide to the ECT Act in South Africa", https://www.michalsons.com/blog/guide-to-the-ect-act/81

Définition

▪ Une signature électronique doit comporter deux **ensembles de données**, qui sont « apposés, incorporés ou associés de façon logique » et le signataire doit avoir eu **l'intention** qu'un de ces ensembles de données constitue sa signature.

▪ Le terme « données » s'entend de la représentation électronique d'informations sous quelque forme que ce soit. Un message de données peut constituer une signature électronique sous réserve, toutefois, de quelques restrictions.

Restrictions

▪ Les définitions exposées ci-dessus sont soumises aux restrictions suivantes:

- la méthode utilisée pour la signature électronique doit permettre d'**authentifier** le signataire et de démonter qu'il a **approuvé** la signature ; et
- cette méthode doit être **suffisamment fiable** au regard des circonstances.

▪ Autre restriction à prendre en compte : il est impossible d'avoir recours à la signature électronique s'il a été convenu, dans un contrat par exemple, d'utiliser un autre type de signature.

Consentement électronique

▪ Pour certaines transactions, une signature n'est pas obligatoire, car l'existence d'un consentement est considéré suffisante. C'est ainsi qu'aux termes de la loi ECT :

- lorsque les parties à une transaction électronique n'ont pas convenu d'utiliser une signature électronique,
- l'expression de leur intention par voie électronique est valable,
- bien qu'il ne s'agisse pas d'une signature électronique.

▪ Pour ces transactions, il n'est nul besoin d'une signature électronique, et un consentement électronique est suffisant.

Signatures électroniques avancées

▪ La signature électronique peut revêtir différentes formes : elle peut être simple ou avancée. La signature électronique avancée **(5)** a été créée par loi ECT, et n'est pas prévue par la common law. Ces deux types de signature se distinguent de plusieurs points. Notamment, contrairement aux signatures électroniques simples, la délivrance du certificat accompagnant la signature électronique avancée est conditionnée à l'authentification du bénéficiaire en face-à-face.

▪ La loi ECT dispose que la signature électronique avancée doit résulter d'un processus qui a été accrédité par une autorité compétente, à savoir le ministère des communications. Pour le moment, seules deux organisations ont été accréditées pour la fourniture de signatures électroniques avancées en Afrique du Sud. Il faut noter que des textes de loi (issus du droit primaire ou secondaire) peuvent exiger l'utilisation d'une signature électronique avancée dans certaines situations.

▪ Enfin, la principale différence entre une signature électronique avancée et une signature électronique simple tient à leurs effets juridiques : seule la signature électronique avancée bénéficie d'une présomption de validité.

(5) "Guide to Advanced Electronic Signatures", Michalsons, https://www.michalsons.com/blog/guide-to-advanced-electronic-signatures/193

DAVID LUYT

A practical overview of electronic signature in South Africa

▪ *Electronic signatures are coming of age in South Africa, with early adopters transitioning their existing paper-based processes to the digital environment and making huge savings in efficiency and gains in reliability as a result. Many international digital transaction management service providers have made landfall in the country and are slowly gaining a foothold, while local developers are coming up with innovative electronic signature solutions suited to the African context.*

▪ *Electronic signatures have been legal in South Africa for more than a decade. The accreditation of advanced electronic signature providers in 2012 saw a surge of renewed interest. Recent case law from 2014 confirmed and applied the relevant legislation for the first time.*

▪ *We believe that as a developing nation plagued by corruption, poor service delivery, and negative international perceptions – there is a great need for certainty.*

▪ *We use handwritten signatures because we think that they provide this certainty. But, this is a false comfort. Handwritten signatures are unreliable, easy to forge, and readily disputed. Testimony from handwriting experts is a notoriously unreliable way of upholding a signature, because the other side will typically appoint their own handwriting expert to dispute your evidence. Witnesses leave companies, die, or otherwise disappear.*

▪ *There are many better methods of achieving certainty about who people are and what they intend that have been developed for electronic signatures, including email verification, two-factor authentication, and PKI encryption. Modern electronic authentication methods used in electronic signatures are far superior and have much less scope for disputes of fact.*

Laws

▪ *Three sets of laws regulate electronic signatures for any given transaction under South African law:*

- *the South African common law (Roman Dutch law and past court decisions);*
- *the ECT Act (Electronic Communications and Transactions Act 25 of 2002) (**1**); and*
- *legislation specific to that type of transaction.*

(1) http://www.gov.za/sites/www.gov.za/files/a25-02.pdf

Common Law

▪ *South African courts have stated in past decisions that the meaning of signature is its ordinary dictionary definition, namely: the name of the person written in their own hand as an authentication of a document or writing.*

▪ *The essential elements of this definition are:*

- *it must be the **name or mark** of the person signing;*
- *the person signing must have **applied it themselves**; and*
- *the person signing must have **intended** it to **authenticate** them.*

▪ *This means that if a signature fulfils this definition it is a signature for the purposes of the common law. Our lawmakers have not explicitly excluded electronic signatures from the common law of signatures. This means that the common law applies to electronic signatures.*

Functional approach

▪ *When assessing whether something constitutes a signature, the courts have tended to focus on the intention of the parties. If the parties intended something to be their signature, then it will generally be held to be a signature in terms of the common law.*

▪ *The courts have found that if a signature is required, it does not have to be a handwritten signature and an electronic signature will be sufficient, if the intention requirement is met.*

▪ *So, an electronic signature meets the common law definition of a 'signature', because:*

- *the signing person's signature contains their **name** (or another way of identifying them);*
- *the signing person **applies it themselves** by choosing to apply it to a document; and*
- *the signing person **intended** the signature to **authenticate** them.*

Past decisions

▪ *The South African case of Spring Forest Trading v Wilberry **(2)** confirmed the functional approach, where the Supreme Court of Appeal held that the parties had validly cancelled a contract by email signed with an electronic signature.*

(2) http://www.saflii.org/za/cases/ZASCA/2014/178.html

▪ *The contract between the parties stated that any changes to the contract had to be **in writing** and **signed** by the parties.*

▪ *According to the ECT Act, a requirement that a document must be in writing, "is met if the document or information is […] in the form of a data message", and an agreement "is not without legal force and effect*

merely because it was concluded […] by means of data messages". As emails are a form of data message, the court found that this satisfied the 'in writing' requirement of the contract.

- *The ECT Act also defines an electronic signature as including "data attached to […] or logically associated with other data and which is intended by the user to serve as a signature". The court found that, in the case of emails, the typed names at the end of the emails satisfied the 'signed' requirement of the contract, because the names served to authenticate the identities of the parties contacting one another.*
- *As both of the requirements were met, the court held that the emails did indeed amount to a valid change to the contract, and the contract had been cancelled* ***(3)****.*

(3) « Spring Forest Trading v Wilberry, Michalsons», https://www.michalsons.com/blog/spring-forest-trading-v-wilberry/14861

ECT Act

- *The ECT Act regulates many electronic communications and transactions* ***(4)****. It essentially confirms the common law positions and states that electronic signatures are valid signatures despite being in electronic form.*

(4) "Guide to the ECT Act in South Africa", https://www.michalsons.com/blog/guide-to-the-ect-act/81

Definition

- *The definition in the Act states that an electronic signature must involve* ***two sets of data****. Those two sets of data must have a* ***relationship*** *where they are "attached to, incorporated in, or logically associated" with each other and the signing person must have had the* ***intention*** *that one of these sets of data be their signature.*
- *In terms of this Act, 'data' means electronic representations of information in any form. There are some requirements for a data message to meet to be an electronic signature.*

Restrictions

- *The Act has certain restrictions with which a data message must comply to be an electronic signature:*
  - *the electronic signature technology must somehow* ***authenticate*** *the signatory and show that they* ***approved*** *the signature; and*
  - *this method must be* ***sufficiently reliable*** *in the circumstances.*
- *You also cannot use an electronic signature if you have* ***agreed to use another type*** *of signature, for example through a contract.*

Electronic consent

▪ *If you are entering transactions where consent is sufficient and a signature is not required, then you don't need to use an electronic signature. The Act says that:*

- *where the parties to an electronic transaction have **not agreed** to use an electronic signature;*
- *an **electronic expression of intention** is valid;*
- *despite not **being an electronic signature**.*

▪ *For those transactions, electronic consent will be sufficient.*

Advanced electronic signatures

▪ *Advanced electronic signatures **(5)** are legally different from ordinary electronic signatures. They were created by the ECT Act and do not exist in common law. The Act says that it must be from a **process accredited** by the **Department of Communications** (which is the relevant Authority). The current accredited process involves face-to-face authentication of the person to whom the advanced electronic signature certificate is issued as the time of issuing, which is not required when it comes to ordinary electronic signatures.*

▪ *Only two organisations have been accredited to provide advanced electronic signatures in South Africa.*

▪ *You must use an advanced electronic signature when a law requires a signature. Laws include both primary and subordinate legislation.*

▪ *The major difference between the legal effects of an advanced electronic signature as opposed to an ordinary electronic signature is that there is an evidentiary presumption that applies to advanced electronic signatures and not to ordinary electronic signatures.*

(5) "Guide to Advanced Electronic Signatures", Michalsons, https://www.michalsons.com/blog/guide-to-advanced-electronic-signatures/193

DAVID LUYT

Focus sur la signature électronique à distance

▪ Le règlement européen n°910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (dit « **règlement eIDAS** ») est directement applicable depuis le 1 juillet 2016 dans tous les États membres de l'Union européenne, et donc en Allemagne. Ce règlement, qui vise à harmoniser le régime des signatures électroniques, a été plutôt bien accueilli par les sociétés et associations allemandes **(1)**. Ses dispositions viennent notamment préciser les règles en matière de signatures électroniques à distance.

La signature électronique à distance

▪ La différence entre une signature électronique à distance et une signature électronique « traditionnelle » réside dans **l'emplacement du dispositif de création de signature**. Avec une signature électronique simple, la signature est créée dans un environnement géré par le signataire, par exemple une carte et un lecteur de carte. En revanche, une signature électronique à distance est créée à l'extérieur cet environnement, sur un matériel sécurisé géré par un prestataire de services de confiance. Dans ce cas de figure, le signataire peut lancer la procédure de signature à distance simplement au moyen d'un dispositif intelligent (une tablette ou un téléphone portable par exemple). La signature électronique à distance est notamment utilisée dans le secteur bancaire pour réaliser des transactions monétaires : le client d'une banque télécharge et installe sur son appareil mobile une application, grâce à laquelle et il peut ensuite transférer de l'argent à distance.

▪ Le champ d'application de la signature électronique à distance est toutefois limité en Allemagne, faute de reconnaissance légale. Le principe en droit allemand est celui du consensualisme, et les parties peuvent conclure un contrat juridiquement contraignant simplement en exprimant leur consentement à cette opération et leur intention d'être liée par celle-ci. Ce consentement peut tout à fait se manifester par l'apposition d'une signature électronique à distance. Par exception, pour certaines opérations, la force contraignante du contrat est subordonnée à une signature manuscrite, et ce non seulement dans le but de protéger les parties contractantes contre

(1) Wulff, Marianne : Avis du groupement de travail fédéral des prestataires de services informatiques locaux. (Vitako), 01.11.2016, accessible (en allemand) par le lien http://www.vitako.de/Publikationen/Vitako-Stellungnahme%20eIDAS-Durchf%C3%BChrungsgesetz.pdf

des décisions imprudentes, mais également de préserver les éléments de preuve en cas de procédures judiciaires (2). Dans ces situations, aux termes de la loi allemande sur la signature numérique (la « SigG ») (3), seule une **signature électronique qualifiée** sera réputée juridiquement équivalente à une signature manuscrite. Pour la SigG, le dispositif de création de signature doit être sous le contrôle du signataire (4). C'est la raison pour laquelle, en Allemagne, une signature électronique à distance n'est pas reconnue comme équivalente à une signature électronique qualifiée.

(2) Par exemple le contrat de prêt, art. 492 BGB) ou le cautionnement (art. 766 BGB).

(3) Art. 126a § 1, code civil allemand (BGB).

(4) Art. 5 § 6, SigG.

▪ Cette position de la loi allemande s'oppose au règlement européen eIDAS qui attribue, quant à lui, le même effet juridique contraignant à une signature électronique à distance créée par un prestataire de services de confiance qualifié qu'à une signature électronique qualifiée créée dans un environnement géré par le signataire (5). Or, il convient de rappeler qu'en cas de contradiction avec les législations nationales des États membres de l'UE, le règlement eIDAS prime. **La situation actuelle conduit donc à une incertitude juridique** et à l'interrogation suivante : les accords conclus par signature électronique à distance sont-ils juridiquement contraignants, ou bien ne sont-ils pas valables faute de signature électronique qualifiée ? Sur ce point, il sera intéressant de suivre comment les tribunaux appliqueront le règlement eIDAS au regard la loi allemande.

(5) Considérant n°52, règlement eIDAS.

Force probante de la signature électronique à distance

▪ L'article 371a, paragraphe 1, du Code de procédure civile allemand (ZPO) pose, dans son alinéa 1, les règles relatives à la valeur probante des documents électroniques privés portant une signature électronique qualifiée au sens de la SigG et instaure, dans son aliéna 2, une **présomption d'authenticité** au profit de ces documents.

▪ Sur cette question, le règlement eIDAS indique uniquement que 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 (6). Eu égard à sa formulation générale, il pourrait en être déduit que le règlement eIDAS n'a pas d'incidence directe sur l'article 371a du ZPO. Toutefois, puisque, compte tenu de la **primauté du texte européen**, les tribunaux allemands ne doivent plus appliquer la définition de signature électronique qualifiée figurant dans la SigG, mais celle contenue dans le règlement eIDAS (7), et que ce dernier instaure

(6) Art. 25 § 1, règlement eIDAS

(7) Art. 3, § 12, règlement eIDAS

l'équivalence des signatures électroniques qualifiées et des signatures électroniques à distance, les tribunaux allemands seront donc amenés à reconnaître également la valeur probante des signatures électroniques à distance.

▪ Il demeure que la présomption du ZPO n'est actuellement applicable que si le détenteur de la clé de signature est le signataire de la signature électronique qualifiée. Or, cela ne sera justement pas le cas lorsque le signataire appose une signature électronique à distance par l'intermédiaire d'un prestataire de services de confiance qualifié, parce que le détenteur de la clé sera alors le prestataire de services de confiance. En l'absence de précision sur ce point dans le règlement eIDAS, les tribunaux peuvent décider d'appliquer une présomption de preuve différente à l'égard des signatures électroniques à distance. Cette différence pourrait se justifier si une signature électronique à distance était plus vulnérable aux modifications qu'une signature électronique qualifiée, mais puisque les prestataires de services de confiance qui la délivre doivent être qualifiés, ils doivent logiquement satisfaire à des exigences supplémentaires en termes de sécurité.

▪ Il en résulte que **la jurisprudence ou le législateur doit intervenir** afin de clarifier la situation et dissiper l'incertitude juridique qui règne actuellement en Allemagne concernant la force contraignante des contrats conclus au moyen d'une signature électronique à distance.

SUSANNE KLEIN
&
FLORIAN
GROOTHUIS

Focus on remote electronic signatures

▪ *The EU regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market ("**eIDAS-Regulation**") is directly applicable in all EU Member States since July 1st, 2016. German companies and associations **(1)** have responded positively to the eIDAS-Regulation regarding the harmonization of electronic signatures, especially with respect to the creation of remote electronic signatures.*

Remote electronic signatures

▪ *The difference between a remote and a "traditional" electronic signature is the **location of the signature creation device**: When the signatory uses the "traditional" electronic signature the signature itself gets created in the environment of the signatory, i.e. by using a card in combination with a card reader. In contrast, when signing an agreement by using a remote electronic signature such signature gets created externally on a hardware security module which is managed by a trusted provider that is not located in the environment of the signatory. In this case, it is not necessary for the signatory to possess a card and a card reader anymore as it is already sufficient to initiate the procedure remotely through a smart device (i.e. tablet, mobile phone). In Germany, this procedure is partly used in the banking sector for the transaction of money. For this purpose, the customer of a bank needs to download an application, install it on his mobile device and may then transfer the money remotely.*

▪ *However, the application area of remote electronic signatures is limited because of its lack of legal recognition. In general, contracting parties can conclude a legally binding contract under German law through a mutual agreement that expresses the intention of both parties. Because of the lack of any additional requirements this also can be done through a remote electronic signature which is just another way of declaring the individual's will. But, apart from that, the German law requires a handwritten signature for certain declarations as formal requirement for a legally binding declaration to protect the contracting parties from imprudent decisions and to preserve evidence for court procedures **(2)**. In these cases, an electronic signature is accepted as legal equivalent to the written form if it is a*

(1) Wulff, Marianne: Statement of the Federal Working Group of local IT services e.V. (Vitako), 01.11.2016, available (in German) under http://www.vitako.de/Publikationen/Vitako-Stellungnahme%20eIDAS-Durchf%C3%BChrungsgesetz.pdf

(2) e.g. consumer loan agreements pursuant to Sec. 492 BGB, suretyship according to Sec. 766 BGB.

qualified electronic signature *according to the German Digital Signature Act (**SigG**) **(3)**. Whereas the SigG defines whether an electronic signature is qualified, it does not regulate the use of remote electronic signatures. It rather expects the signature creation device to be under control of the signatory **(4)**. The consequence is that remote electronic signatures have not been accepted as equivalent to qualified electronic signatures yet.*

(3) Sec. 126a par. 1 of the German Civil Code (BGB).

(4) Sec. 5 par. 6 SigG.

- *The eIDAS-Regulation on the other hand attributes the same legal binding effect to the remote electronic signature created by a qualified trusted provider as to a qualified electronic signature that has been created in the environment of the signatory **(5)**. Since the eIDAS-Regulation holds precedence when contradictions to national laws of EU-Member States occur, **the current situation leads to legal uncertainty** in Germany about whether agreements that have been concluded via remote electronic signature are legally binding or a qualified electronic signature is still necessary instead. As long as the German law is not adjusted to the eIDAS-Regulation it remains to be seen how German courts will apply the eIDAS-Regulation.*

(5) Recital 52 eIDAS-Regulation.

German case law on electronic signatures

- *In addition, the courts have to deal with electronic signatures pursuant to Sec. 371a par. 1 (1) of the German Code of Civil Procedure (ZPO). According to this provision the rules concerning the evidentiary value of private records and documents shall be applied to private electronic documents bearing a qualified electronic signature pursuant to the SigG. Furthermore, Sec. 371a par. 1 (2) ZPO provides a **prima facie evidence** in regards to the authenticity of the declaration for the benefit of the holder of the signature key.*

- *In this regard, the eIDAS-Regulation only determines that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the ground that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures **(6)**. As the eIDAS-Regulation does not contain more detailed rules about the evidentiary value of electronic signatures, it does not have a direct impact on the procedural rules of Sec. 371a ZPO. Nevertheless, Sec. 371a ZPO will indirectly be influenced since the **German courts** cannot apply the definition of a qualified electronic signature according to the SigG anymore. They rather **have to apply the definitions of the eIDAS-Regulation (7)**. And as the eIDAS-Regulation accepts the equivalence of qualified*

(6) Article 25 par. 1 eIDAS-Regulation

(7) Article 3 No. 12 eIDAS-Regulation

electronic signatures and remote electronic signatures the German courts need to accept their evidentiary value, too.

- *However, the problem remains that the prima facie evidence is currently only applicable for the holder of the signature key being the signatory of a qualified electronic signature. This won´t be the case though when the signatory signs remotely through a qualified trusted provider because the key holder will be the trusted service then. Since the eIDAS-Regulation does not regulate the procedural application of electronic signatures more specifically the courts may apply a different prima facie standard for remote electronic signatures. This might be appropriate if a remote electronic signature was more vulnerable for manipulation than a qualified electronic signature, but should in general not be the case since the trusted service providers must be qualified and, therefore, fulfil additional security procedures.*

- ***The current legal uncertainty** whether agreements that require by law a qualified electronic signature are legally binding when they have been concluded via a remote electronic signature instead **can only be clarified by court practice or a new German legislation**.*

SUSANNE KLEIN
&
FLORIAN
GROOTHUIS

Signature électronique et processus de vente en ligne

▪ Depuis des années, la signature électronique s'annonce pleine de promesses : rapidité, flexibilité, simplicité, sécurité juridique… Depuis la transposition de la directive 1999/93/CE dans le code civil belge et dans la loi du 9 juillet 2001 « signatures électroniques » (maintenant abrogée et incorporée dans le Code de droit économique), la signature électronique ne peut être écartée par le juge saisi d'un litige. Celui-ci doit apprécier dans les faits quel est l'effet de cette signature. Si celle-ci correspond aux conditions prévues dans la loi, elle sera considérée comme équivalente à une signature manuscrite. Le règlement (UE) n°910/2014 dit « eIDas » précise et améliore ce cadre juridique.

(1) Mougenot, D., « Preuve », Rép. not., Tome IV, Les obligations, Livre 2, Bruxelles, Larcier, 2012, n° 121-3.

▪ La carte d'identité belge contient également les certificats nécessaires pour permettre la signature par le biais d'une signature électronique qualifiée, qui assure la meilleure sécurité juridique. **Dans les faits** toutefois, **la signature manuscrite reste toujours la norme en Belgique et le recours à une signature électronique qualifiée pour signer un document**, comme un contrat, **reste rare**, voire inexistant.

▪ On constate que, bien que de très nombreuses transactions se fassent en ligne sur les sites d'e-commerce, elles se font sans le recours à la signature électronique « traditionnelle ». Afin d'assurer la sécurité juridique des transactions en l'absence de cette signature, les commerçants doivent mettre en place tout un processus (le ***checkout funnel***) qui leur permettra d'identifier l'auteur d'une commande, de contrôler l'accord de celui-ci sur les conditions de la commande et de se ménager la preuve de la transaction (les fonctions usuelles de la signature). Bien souvent, le risque du commerçant est mitigé par le paiement immédiat du client via prélèvement sur sa carte de crédit. Dans l'énorme majorité des cas, les litiges ne portent d'ailleurs pas sur la réalité de la commande en ligne.

▪ L'exigence de rapidité et la difficulté pratique de multiplier les étapes d'encodage de coordonnées liées à l'usage des smartphone pour passer commande ou même pour accepter un document remet toutefois en cause ce *checkout funnel*, que les commerçants veulent raccourcir, voire supprimer (achats *one-click).* **La signature électronique revient donc sur le devant de la scène**.

▪ Le recours à la carte d'identité électronique implique un **lecteur de carte** et n'est pas vraiment pratique. De même en ce qui concerne l'utilisation d'une **authentification à double facteur**, comme un numéro aléatoire généré par une application tierce ou un appareil. Le **dessin** d'une signature sur l'écran ne présente guère de garantie quant à l'identification du signataire. Les outils de reconnaissance biométriques, dont sont désormais équipés la plupart des smartphones et ordinateurs, semblent par contre plus prometteurs. Par définition, la **biométrie** permet d'identifier une personne et remplit donc la fonction d'identification. Par sa mise en œuvre appropriée dans le cadre d'une commande, la signature biométrique pourrait également manifester l'adhésion du signataire au contenu signé. La signature pourrait être conservée et servir de preuve de la transaction.

▪ Bien que très intéressante pratiquement, les informations biométriques sont des **données à caractère personnel** qui doivent être traitées avec soin et précaution. En effet, un mot de passe peut être modifié, pas ses empreintes digitales. La Commission de Protection de la Vie Privée a émis un avis important à cet égard **(2)**.

(2) CPVP, Avis d'initiative relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes (A/2008/017), 9 avril 2008

ALEXANDRE CASSART

Electronic signature and online sales process

▪ *For years, electronic signatures have been promising but not delivering: speed, flexibility, simplicity, legal certainty... Since the transposition of Directive 1999/93/EC into the Belgian Civil Code and in the law of 9 July 2001 (now repealed and incorporated into the Code of Economic Law), electronic signature cannot be excluded by Courts because it is electronic. Court must assess the validity of that signature. If it meets the legal definitions and functions, it will be considered equivalent to a handwritten signature. Regulation (EU) No 910/2014, known as eIDas, clarifies and improves this legal framework.*

▪ *The Belgian identity card contains the necessary certificates to allow the signature by means of a qualified electronic signature, which ensures the best legal certainty. **In practice, however, handwritten signature is still the norm in Belgium and the use of a qualified electronic signature to sign a document,** such as a contract, **remains rare** or non-existent.*

▪ *It can be seen that, although many transactions are carried out online on e-commerce sites, they are done without the use of the "traditional" electronic signature. In order to ensure the legal security of transactions in the absence of this signature, traders must put in place a whole process (the **checkout funnel**) which will allow them to identify the author of an order, to control the agreement of the latter on the conditions of the order and to take care of the proof of the transaction (the usual functions of the signature). Often, the risk of the merchant is mitigated by the immediate payment of the customer via his credit card. In the vast majority of cases, disputes do not concern the reality of online ordering.*

▪ *The requirement of speed and the practical difficulty of multiplying the steps in case of use of smartphones to place an order or even to accept a document calls into question this checkout funnel, which the traders want to shorten, or even suppress (one-click purchases). **The electronic signature is then back on the scene**.*

(1) Mougenot, D., « Preuve », Rép. not., Tome IV, Les obligations, Livre 2, Bruxelles, Larcier, 2012, n° 121-3.

▪ *The use of the electronic ID card involves a* ***card reader*** *and is not really practical. The same applies to the use of* ***double-factor authentication****, such as a random number generated by a third-party application or device. To* ***draw*** *a signature on the screen does not offer enough guarantee as to the identification of the signatory. The* ***biometric recognition*** *tools, which are now equipped with most smartphones and computers, seem more promising. By definition, biometrics makes it possible to identify a person and thus fulfills the identification function. By its proper implementation within the order process, the signature biometric could also manifest the adhesion of the signatory to the signed content. The signature could be retained and serve as proof of the transaction.*

▪ *Although very interesting practically, biometric information is* ***personal data*** *that must be treated with care and precaution. Indeed, a password can be changed, not one's fingerprints. The Belgian Commission for the Protection of Privacy has issued an important opinion in this regard* ***(2)****.*

(2) CPVP, Avis d'initiative relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes (A/2008/017), 9 April 2008

ALEXANDRE CASSART

La « French touch » pour la signature électronique

▪ Avec l'intensification des échanges électroniques et de la transformation numérique des entreprises, la signature électronique est en vogue surtout dans le secteur de la banque et de l'assurance. Difficile, compliquée? Non, la signature électronique est simple et vise tout le monde, l'essayer, c'est l'adopter !

▪ Introduisant les dispositions de la **Directive européenne de 1999**, la loi de 2000 adaptant le droit de la preuve aux technologies de l'information et relative à la signature électronique a révolutionné le Code civil français.

▪ Applicable à partir du 1er juillet 2016, le **Règlement eIDAS (1)** est une véritable révolution juridique dans le monde de la dématérialisation. d'une part, il permet de franchir une nouvelle étape dans le droit de la signature électronique en définissant des règles communes applicables sur l'ensemble de l'Union ; et d'autre part, il définit un droit des prestataires de confiance: définition des prestations, modalités communes de qualification et critères transnationaux de reconnaissance.

▪ Modifié à la marge en octobre 2016 à l'**article 1367 al. 1** du nouveau Code civil, le droit français s'attache tout d'abord à décrire les fonctions d'une **signature** quel que soit son support ou son procédé manuscrit ou électronique :

- perfection ou concrétisation d'un acte juridique ;
- identification du signataire et donc de l'origine d'un acte ;
- manifestation du consentement des parties qui s'obligent à l'acte qu'elles ont signé ;
- authenticité, lorsque l'auteur de la signature est un officier public, gage de confiance.

▪ Selon l'**article 1367 al. 2** du Code civil, 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. On retrouve ici les fonctions décrites ci-dessus. Le stylo est remplacé par un « procédé fiable » qui doit garantir l'identification du signataire et l'intégrité de l'acte signé, c'est-à-dire l'impossibilité d'altérer l'acte.

▪ **La difficulté de la signature électronique est qu'en pratique, on ne la voit pas :** c'est généralement un code obtenu à partir d'une fonction de hachage qui va sceller un document avec une signature et repose sur l'utilisation d'un certificat électronique. Le plus souvent, les documents électroniques au format Pades qui sont autoporteurs de la signature électronique, permettent de vérifier facilement qu'un document est signé (coche verte indiquant que la signature est valable, visualisation du certificat électronique avec mention de l'identité du signataire et de l'horodatage).

REFERENCES

(1) Règlement (UE) no 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 et abrogeant la directive 1999/93/CE, dit Règlement eIDAS pour e-IDentity And Signature.

(2) Art. R249-10 du Code de procédure pénale : La signature électronique n'est valablement apposée que par l'usage d'un procédé qui permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte.
Elle doit être sécurisée au sens du 2 de l'article 1er du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil relatif à la signature électronique.

(3) Art. 322 du Code des douanes.

(4) Art. L. 212-3 du Code des relations entre le public l'administration.

(5) Art. L.1111-28 al.2 du Code de la santé publique : « Lorsque le document sur lequel la

▪ Ne sont pas une signature électronique : une signature manuscrite sur un écran, une signature scannée. Une signature graphique digitale de nature hybride, appelée en droit pénal « **signature numérique** » est en revanche considérée comme valable :elle consiste dans l'apposition d'un dessin de signature sur une tablette graphique ou tactile pour en obtenir une image numérique ; sa fiabilité technique est garantie par un dispositif sécurisé, impliquant un scellement unique de ce graphique avec le document électronique signé et une authentification forte du signataire garantissant garantie d'origine et d'intégrité.

▪ Certains textes spécifiques ont intégré la signature électronique en dehors du droit civil commun des actes sous signature privés, comme par exemples en droit fiscal avec la signature de la facture électronique, en droit pénal **(2)** et droit douanier **(3)**, en droit administratif **(4)** et récemment en janvier 2017 en droit de la santé **(5)**, et enfin la signature électronique des actes authentiques par les notaires et les huissiers de justice **(6)**.

▪ Mais n'ayons pas peur, à défaut de texte spécifique, le droit commun du Code civil et du règlement eIDAS pour la signature électronique s'appliquera.

▪ Aux côtés, de la signature électronique, le règlement eIDAS a introduit dans notre droit le cachet électronique. Il sert à prouver qu'un document électronique a été délivré par une personne morale en garantissant l'origine et l'intégrité du document. Cette notion de cachet électronique est une semi-nouveauté pour le droit français, puisqu'elle n'existait que dans le Référentiel général de sécurité (RGS) pour les administrations publiques. A noter que le droit suisse, vient de la consacrer, ce qui permettra un « raccordement » avec les pays de l'Union européenne.

Niveaux de fiabilité technico-juridique

▪ La signature électronique présente différents niveaux, non de validité, mais de fiabilité technico-juridique et de sécurité.

1er niveau : la signature électronique simple

▪ Sur le niveau « **simple** », c'est à celui qui a fourni l'outil de signature électronique à son cocontractant, de prouver la fiabilité de son procédé **(7)**. En pratique, cela nécessitera de mettre en place des éléments de sécurisation juridique complémentaires : garanties contractuelles du prestataire de signature électronique, audit de conformité, legal opinion, une politique d'identification électronique, une convention de preuve et documents de gestion des preuves associés.

▪ Le niveau de signature électronique « simple » a parfaitement été reconnu comme valable par la jurisprudence française, notamment par la Cour de cassation pour les contrats d'assurance **(8)**

▪ Toutefois, ce niveau n'est pas exactement identique à celui du règlement eIDAS, lequel est largement moins exigeant que la française. **(9)**

signature est apposée est créé sur un support numérique, le procédé de signature respecte les conditions du second alinéa de l'article 1367 du code civil. »

(6) Art. 1367 du Code Civil

(7) L'article 1er du décret du 30 mars 2001 définit la signature électronique comme « une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1367 du Code civil ». Les données de création de signature électronique sont définies par ailleurs comme « les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique ».

(8) « L'assurance assure avec la signature électronique en ligne », Polyanna Bigle www.alain-bensoussan.com, 22-6-2016.

(9) Le règlement définit ainsi la signature électronique comme « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le

2e niveau : la signature électronique sécurisée

▪ La signature électronique **sécurisée** doit satisfaire aux conditions de la signature électronique simple ainsi qu'à des exigences supplémentaires prévues par l'article 1er du décret précité :

- « être propre au signataire ;
- « être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- « garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ».

▪ Le législateur français n'a pas cru bon de profiter de la réforme du code civil d'octobre 2016 pour modifier la dénomination en cohérence avec le règlement eIDAS qui prévoit la signature électronique « **avancée** ». Toutefois, ici les exigences sont similaires au droit français. **(10)**

▪ La différence avec le droit français réside dans le c) de l'article 26 du Règlement : le contrôle exclusif des données de création de la signature peut être réalisé « avec un niveau de confiance élevé ». In fine, cela assouplit la notion de droit français **(11)** de « contrôle exclusif », pour permettre – semble-t-il – la signature électronique avancée réalisée « à distance ».

▪ L'intérêt de la signature électronique sécurisée ou avancée, réside dans le fait que la **charge de la preuve** de la fiabilité du procédé est allégée de part des mécanismes de sécurité qu'elle doit mettre en œuvre.

▪ En pratique, les difficultés résident dans le fait qu'il n'existe pas de label ou de certification officielle permettant de s'assurer que la signature électronique est de niveau sécurisé ou avancé. Cela nécessitera là encore de mettre en place des éléments de sécurisation juridique complémentaires précités.

3e niveau : la signature électronique présumée fiable

▪ Selon l'article 2 du décret précité, une signature électronique est **présumée fiable** lorsque « ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié ». **(12)**

▪ L'intérêt de la présomption de fiabilité réside dans le renversement de la **charge de la preuve** : c'est à celui qui conteste la signature électronique d'apporter la preuve technique que les dispositifs de création de la signature ou que le certificat électronique qualifié sont défaillants.

▪ Le règlement eIDAS parlera quant à lui de la signature électronique **qualifiée**, aux exigences similaires à la présumée fiable de droit français. **(13)**

signataire utilise pour signer (Art. 3.10 du Règlement eIDAS).

(10) « Une signature électronique avancée satisfait aux exigences suivantes :
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. » (Art. 26 du Règlement eIDAS et sa décision exécution 2015-1506 08 09 2015 signature électronique avancée cachet spécification technique format identification transaction 910-2014)

(11) Provenant elle-même de la Directive de 1999

(12) Le certificat électronique qualifié est un « un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire » qui doit répondre à certaines exigences techniques et

▪ Il est intéressant de noter que le règlement eIDAS va plus loin que la présomption de droit français en ce qu'il institue deux principes :

- équivalence : la signature électronique qualifiée a le même effet juridique qu'une signature manuscrite
- non-discrimination : la signature ne peut être refusée en justice pour la seule raison qu'elle est électronique ou qu'elle n'est pas « qualifiée »

Statut et un label de confiance

▪ Le règlement eIDAS, d'application directe dans tous les pays de l'Union européenne depuis le 1er juillet 2016, a pour objectif de compléter la législation actuelle et d'étendre la reconnaissance et l'acceptation mutuelles de l'identification, de l'authentification et des signatures électroniques.

▪ Il crée également un statut commun instaurant un organe de contrôle national dans chaque Etat membre ainsi qu'un label de confiance pour les prestataires de services de confiance (dits **PSCO**) : pour bénéficier de ce label les PSCO devront obtenir une qualification qui sera reconnue dans l'UE. Ils bénéficieront d'une présomption de fiabilité de leurs services mais seront également présumés fautifs en cas de difficultés liées au service de confiance.

Impacts

▪ Malgré la standardisation européenne permettant de choisir, en confiance, des offres diversifiées des PSCO dans toute l'Europe, deux difficultés sont à lever dans a mise en œuvre d'un projet de signature électronique :

- premièrement **la spécificité des exigences de droit français** entourant à la fois tel ou tel acte juridique, et le processus de conclusion de cet acte ;
- deuxièmement, **l'absence de règles uniques ou uniformes à l'international** sur la signature électronique à l'heure pourtant de la mondialisation des échanges et des transactions, fait peser le spectre de la remise en cause des actes signés électroniquement dans un autre pays.

Conclusion

▪ En conclusion, la signature électronique est un outil juridique et technique valable en droit français et européen. **(14)**

▪ Néanmoins, une analyse de risques juridiques mais aussi techniques, est un prérequis indispensable à la mise en œuvre d'un projet de signature quel qu'il soit. Ne pas le faire pourrait déclencher le « NO GO » du projet et surtout la mise en péril de l'activité de l'entreprise par remise en cause de la validité des documents. Enfin, les solutions de sécurisation juridiques complémentaires sont recommandées pour parer l'éventuelle remise en cause technique d'une signature électronique.

être délivré par un prestataire de services de certification électronique (PSCE).

(13) il s'agit d' « 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 qualifié de signature électronique ».

(14) Pour en savoir plus sur la signature électronique : Archimag, guide pratique n°53, « Droit de l'information », novembre 2015.
Voir également sur le site www.alain-bensoussan.com : « Règlement eIDAS sur l'identification pour les transactions électroniques », Polyanna Bigle et Eric Barbry, 19-04-2016 ; et « Signature électronique en Europe : nouvelle étape », Polyanna Bigle 17-09-2014.

POLYANNA BIGLE

The French touch for electronic signatures

▪ *With the intensification of electronic exchanges and the digital transformation of companies, electronic signature is booming, especially in the banking and insurance sector. Difficult, complicated? No! The electronic signature is simple and for everyone. Try It! You'll like it!*

▪ *The **1999 European Directive**, introduced into French law by the 2000 Act adapting the law of evidence to information technologies and relating to the electronic signature, drastically changed the Civil Code.*

▪ *The **eIDAS Regulation (1)**, applicable since 1 July 2016, was yet another legal revolution in the digital world. It not only tooks a new step forward in electronic signature law by defining common rules applicable across the Union, but also established a framework for trust service providers: definition of services, common qualification procedures and transnational criteria for recognition.*

▪ *Marginally amended in October 2016, **Article 1367(1)** of the French Civil Code describes the functions of a **signature**, whether handwritten or electronic, regardless of its medium or process:*

- *it perfects a legal act;*
- *it identifies its author, the signatory (and thus the origin of the act signed);*
- *it demonstrates the consent of the parties to be bound by the obligations which stem from that act;*
- *it confers authenticity (mark of trust) on the act, where the signatory is a public official.*

▪ *According to **Article 1367(2)** of the Civil Code, the **electronic signature** is a "reliable process of identification which guarantees its relationship with the act to which it is attached." This definition of electronic signature meets the signature functions just described above. Here, the pen is replaced by a "reliable process" that must guarantee the identification of the signatory and the integrity of the act signed (meaning that it should not be possible to alter the act).*

▪ ***The thing with the electronic signature is that in practice we do not see it**: it is generally a code obtained from a hash function that will seal a document with a signature and is based on the use of an electronic certificate. Most the time, electronic documents that are in the PAdES format, which are supporting the electronic signature, make it easy to verify that a document is signed (green check mark indicating that the signature is valid, display of the electronic certificate with details on the identity of the signatory and the timestamp).*

REFERENCES

(1) Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, known as the "eIDAS" Regulation (standing for e-IDentity And Signature).

(2) Art. R249-10 of the Code Criminal Procedure: The electronic signature is validly affixed only by the use of a process which allows the identification of the signatory, guarantees the link of the signature with the act to which it is attached and ensures the integrity of that act.
It must be secure within the meaning of Article 1(2) of decree No. 2001-272 of 30 March 2001 adopted for the application of Article 1316-4 of the Civil Code relating to the electronic signature.

(3) Art. 322 of the Customs Code.

(4) Art. L. 212-3 of the Code governing the relationships between citizens and the administration.

(5) Art. L.1111-28(2) of

▪ *Note that a handwritten signature on a screen or a scanned signature are* not *an electronic signature. In contrast, a hybrid digital graphic signature, referred to under penal law as "**digital signature**", is considered valid: it consists in affixing a signature drawing on a graphic or tactile tablet to obtain a digital image; its technical reliability is guaranteed by a secure device, involving a unique seal of this graph with the electronic document signed and a strong authentication of the signatory guaranteeing its origin and integrity.*

▪ *On top of the standard rules for private signed documents, many sector-specific provisions are also regulating electronic signatures: for example tax law (signature of electronic invoice), criminal law **(2)**, customs law **(3)**, administrative law **(4)** health law **(5)**, and the special provisions on the electronic signature of authenticated instruments by notaries and bailiffs **(6)**.*

▪ *But no need to worry: in the absence of specific text, the general law enshrined in the Civil Code and the eIDAS regulation for the electronic signature will apply.*

▪ *In addition to the electronic signature, the eIDAS regulation introduced the **electronic seal**. It is used to ensure the origin and integrity of an electronic document issued by a legal entity. The concept of electronic seal is a semi-novelty for French law, as it previously existed, but only in the General Security Reference System (Référentiel général de sécurité or "RGS") for public administrations. It should also be noted that Switzerland has just recently established the same concept into its law; this will allow a "connection" with the European Union Member States.*

Levels of technical and legal reliability

▪ *In France, an electronic signature can have different levels — which should be understood not as levels of validity, but as levels of technical and legal reliability and security.*

Level 1: Simple Electronic Signature

▪ *With a "**simple" electronic signature**, it is up to the person who provided the e-signature tool to prove the reliability of that process **(7)**. In practice, this **burden of proof** will require additional legal safeguards, such as contractual guarantees from the electronic signature provider, compliance audit, legal opinion, an electronic identification policy, rules of evidence and related evidence management documents.*

▪ *The simple electronic signature has been recognized as perfectly valid by French case law, in particular by the Cour de Cassation regarding insurance contracts **(8)**.*

▪ *The French "simple electronic signature" is not exactly identical to the ordinary "**electronic signature**" provided for by the eIDAS regulation, as EU rules are far less demanding than French rules on this point. **(9)***

the Public Health Code: "Where the document to which the signature is affixed is created on a digital medium, the signature procedure shall comply with the conditions of the second paragraph of Article 1367 of the Civil Code."

(6) Art. 1367 of French Civil Code

(7) Article 1 of decree of 30 March 2001 defines the electronic signature as "data that results from the use of a process meeting the conditions defined in the first sentence of the second paragraph of Article 1367 of the Civil Code". The electronic-signature-creation data is further defined as "the signatory's specific elements, such as private cryptographic keys, used by him to create an electronic signature".

(8) "L'assurance assure avec la signature électronique en ligne", Polyanna Bigle www.alain-bensoussan.com, 22-6-2016.

(9) Under the eIDAS Regulation "electronic signature" means "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the

Level 2: Secure Electronic Signature

▪ *A **secure electronic signature** must meet the requirements of the simple electronic signature plus additional requirements provided for in Article 1 of the decree of 30 March 2001, namely:*

- *"it is specific to the signatory;*
- *"it is created by means that the signatory can create under his sole control;*
- *it guarantees a link with the act to which it is attached in such a way that any subsequent change in the act is detectable".*

▪ *The eIDAS Regulation uses the term "**advanced" electronic signature**. While the French legislator did not see fit to take advantage of the October 2016 reform of the Civil Code to harmonize the French term with the EU term, the requirements applying to that type of signature are similar in the French and EU provisions **(10)**.*

▪ *With a difference: under the Regulation the signature creation data can be used under the signatory's exclusive control "with a high level of confidence" (point (c) of Art. 26). The concept of "sole control" used instead in French law **(11)** is thereby made more flexible, to allow – it seems – the advanced electronic signature to be made "remotely".*

▪ *The advantage of the secure — or advanced — electronic signature is that the **burden of proof** of the reliability of the process is reduced by the security mechanisms it has to meet.*

▪ *In practice, difficulties can be faced as there is currently no official label or certification ensuring that the electronic signature is secure or advanced. In other words, the additional legal safeguards described above for the simple e-signature will also need to be implemented.*

Level 3: Presumed Reliable Electronic Signature

▪ *According to Article 2 of the aforementioned decree of 30 March 2001, an electronic signature is presumed to be reliable when "this process implements a secure electronic signature that it is established by a secure electronic signature creation device, and the verification of such signature is based on a qualified electronic certificate" **(12)**.*

▪ *The advantage of the presumption of reliability lies in the reversal of the **burden of proof**: it is up to the party challenging the electronic signature to provide technical proof that the signature creation device or the qualified certificate for electronic signature is defective.*

▪ *The eIDAS regulation refers to this type of signature as "**qualified" electronic signature**" with requirements similar to those laid down in the French **presumed reliable electronic signature (13)**.*

signatory to sign" (Art. 3.10 of eIDAS Regulation)

(10) "An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and;
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable." (Art. 26 of eIDAS Regulation and its Implementing Regulation Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals (pursuant to Regulation (EU) No 910/2014)

(11) Derived from the 1999 Directive

(12) The qualified electronic certificate is a "document in electronic form attesting the link between the electronic signature verification data and a signatory" which must meet certain technical requirements

▪ *In this respect, it is interesting to note that the eIDAS Regulation goes further than French law in that it introduces two principles:*

- *the principle of equivalence: a qualified electronic signature has the equivalent legal effect of a handwritten signature*
- *the principle of non-discrimination: an electronic signature cannot be denied in legal proceedings solely on the grounds that it is in an electronic form or that it is not "qualified".*

Status and Trust Mark

▪ *The eIDAS Regulation, which has been directly applicable in all EU Member States since 1 July 2016, aims to complement existing legislation and to extend the mutual recognition and acceptance of e-identification (eID), e-authentication and e-signatures.*

▪ *It also creates a common status, establishes a national supervisory body in each Member State, and a trust mark for trust service providers (**TSP**). To benefit from this trust mark, TSPs must obtain a qualification that will be recognized in the EU. They will benefit from a double-edged presumption: their services will be presumed reliable, but will also be presumed to be at fault in the event of difficulties related to their trust services.*

Impacts

▪ *In spite of the European standardization, which enables to confidently choose among the various offers of TSPs throughout Europe, two difficulties still have to removed when implementing an electronic signature project:*

- *first, **the specific requirements to be met under French law** for certain legal instruments and their formation;*
- *second, the absence of single or uniform rules on the electronic signature **at the international level**; in an age of globalization of trade and transactions, this lack raises the specter of the unenforceability of documents signed electronically in another country.*

Conclusion

▪ *In conclusion, electronic signature is a legal and technical tool valid under French and EU laws.**(14)***

▪ *For all that, an analysis of both legal risks and technical risks is a necessary prerequisite for the implementation of any kind of signature projects. Otherwise, the project could be a no-go, the validity of the documents could be challenged, resulting in putting the business in jeopardy. Adopting additional legal security solutions is also recommended to proactively manage technical disputes over an electronic signature.*

and be issued by a Certification Service Provide (CSP).

(13) Under the eIDAS Regulation it is "an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures".

(14) To find out more on electronic signatures, see Archimag, guide pratique n°53, "Droit de l'information", Nov. 2015.
See also on www.alain-bensoussan.com: "Règlement eIDAS sur l'identification pour les transactions électroniques", Polyanna Bigle et Eric Barbry, 19-04-2016; and "Signature électronique en Europe : nouvelle étape", Polyanna Bigle, 17-09-2014.

POLYANNA BIGLE

Panorama de la signature électronique

▪ **Utilité des signatures électroniques.** Instaurer un climat de confiance dans l'environnement en ligne est essentiel au développement économique et social. La signature électronique, qui permet de signer des documents numériques, contribue à ce climat de confiance en offrant (dans la plupart des cas et dans certaines circonstances) le même statut juridique qu'une signature manuscrite **(1)**. La signature électronique est donc utile dans de nombreuses situations ; elle est par exemple nécessaire lors de la transmission des candidatures et des offres sur la plateforme grecque de passation électronique de marchés publics (ESIDIS).

▪ **Le nouveau règlement européen.** En juillet 2016 est entré en vigueur, dans les 28 États membres de l'Union européenne, le nouveau règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. Ce règlement (UE) 910/2014 dit « règlement eIDAS » a abrogé la directive 1999/93/CE sur la signature électronique sur laquelle reposait en grande partie le précédent cadre juridique grec (et notamment le décret 150/2001 de transposition de ladite directive).

▪ Ainsi que l'a souligné la Commission européenne **(2)**, le règlement eIDAS constitue une étape majeure pour créer un environnement réglementaire prévisible qui permettra des interactions électroniques sûres et sans discontinuité entre les entreprises, les particuliers et les pouvoirs publics. Il permet aux particuliers et aux entreprises d'utiliser le système national d'identification électronique de leur pays pour accéder aux services publics en ligne dans d'autres pays de l'UE où l'identification électronique est disponible. Le règlement crée aussi un marché intérieur européen des services de confiance (signatures électroniques, cachets électroniques, authentification de site internet) en garantissant le fonctionnement transnational de ces services et en leur conférant le même statut juridique que les formalités effectuées avec des documents physiques classiques.

▪ **Les principaux changements (3).** Désormais, les certificats de signature électronique ne peuvent être délivrés qu'aux personnes physiques. Les personnes morales doivent, quant à elles, utiliser des

REFERENCES

(1) Certaines exceptions s'appliquent en droit grec, lorsque les signatures électroniques ne peuvent pas être utilisées, par exemple pour la vente de contrats fonciers. A cet égard, le règlement eIDAS n'affecte pas le droit national ou de l'Union relatif à la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales d'ordre formel (art. 2 du règlement).

(2) Trust Services and eID | Marché unique numérique, https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

(3) Questions & Answers on Trust Services under eIDAS | Marché unique numérique, https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas

(4) « cachet électronique » : 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 (possible pour les personnes morales).

(5) « horodatage électronique » : les données sous forme électronique qui relient d'autres données sous forme électronique à un moment donné, en établissant des preuves que ces dernières données existaient à ce moment.

(6) « service d'envoi recommandé électronique » : un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute

certificats de cachet électronique, dont la vocation n'est pas de réaliser une signature mais de garantir l'intégrité et l'origine des données. Les anciens certificats de signature électronique qualifiés précédemment délivrés aux personnes morales ne peuvent donc plus être utilisés. En outre, le règlement eIDAS introduit de nouveaux services de confiance : les cachets électroniques **(4)**, les horodatages électroniques **(5)** (qui associent les données et documents à un instant particulier, les services d'envoi recommandé électronique) **(6)**, ou encore les certificats d'authentification de site internet **(7)** (qui permettent d'assurer aux internautes que le site qu'ils visitent est exploité par une personne morale identifiable avec des informations dignes de confiance).

▪ **Effets juridiques.** Le règlement opère une distinction entre les signatures électroniques **(8)**, les signatures électroniques avancées **(9)** et les signatures électroniques qualifiées **(10)**. Il réaffirme le principe qu'une signature électronique peut être utilisée comme moyen de preuve en justice, et prévoit expressément que 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. Pour le règlement, l'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite. La reconnaissance mutuelle est également la règle : une signature électronique qualifiée qui repose sur un certificat qualifié délivré en Grèce (ou dans un État membre) est reconnue en tant que signature électronique qualifiée dans tous les autres États membres. Les mêmes principes s'appliquent globalement aux cachets électroniques, aux horodatages électroniques, aux données envoyées et reçues à l'aide d'un service d'envoi recommandé électronique, ainsi qu'aux documents électroniques **(11)**.

▪ **Le régulateur.** En Grèce, la commission de régulation des télécommunications et des postes (« EETT »), une autorité administrative indépendante, est chargée de tenir le registre **(12)** qui comprend des informations relatives aux prestataires qualifiés de services de confiance qualifiés dont elle est responsable, ainsi que des informations relatives aux services de confiance qualifiés qu'ils fournissent.

modification non autorisée.

(7) « certificat d'authentification de site internet » : une attestation qui permet d'authentifier un site internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré.

(8) « 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.

(9) « signature électronique avancée » : une signature électronique qui satisfait aux exigences suivantes : 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.

(10) « 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 qualifié de signature électronique.

(11) « document électronique » : tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel.

(12)http://www.eett.gr/opencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatures/EsignProviders.html

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

A practical overview of electronic signature

▪ ***Why electronic signatures matter***: *Building trust in the online environment is key to economic and social development. In simple terms, electronic signatures provide a way to sign digital documents, offering (in most cases and under specific circumstances) same legal standing as a handwritten signature* ***(1)****. Nowadays, use of electronic signatures is also required for the electronic submission of a bid for participation in public procurement tenders through the National Electronic Procurement System (ESIDIS).*

▪ ***The new Regulation***: *In July 2016 the new EU Regulation for electronic identification (eID) and trust services (eTS) came into force, which applies directly across the 28 Member States. The Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market ("eIDAS Regulation") repealed the e-signature Directive 1999/93/EC and essentially replaced the previous Greek legal framework (namely the Presidential Decree 150/2001, which had transposed into Greek legislation the Directive 1999/93/EC).*

▪ *As noted by the European Commission* ***(2)****, the eIDAS Regulation is a milestone to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. It ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available, and it also creates a European internal market for eTS, namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication, by ensuring that they will work across borders and have the same legal status as traditional paper based processes.*

▪ ***Some key changes (3)***: *Certificates for electronic signatures cannot be issued to legal persons anymore. Instead, legal persons can use certificates for electronic seals, whose aim is not to sign but are means to ensure the integrity and origin of data. This*

REFERENCES

(1) Certain exceptions apply, where electronic signatures cannot be used, e.g. for sale of land contracts. According to Article 2 or the eIDAS Regulation, the latter does not affect Greek or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.

(2) Trust Services and eID | Digital Single Market, https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

(3) Questions & Answers on Trust Services under eIDAS | Digital Single Market, https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas

(4) 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity (available to legal entities).

(5) 'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

(6) 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

(7) 'certificate for website

means that former qualified electronic signature certificates issued to legal persons cannot be used anymore. Moreover, the eIDAS Regulation introduces some new eTS, including electronic seals (4), electronic time stamps (5), which are issued to ensure the correctness of the time linked to data and documents, electronic registered delivery services (6) and certificates for website authentication (7), which are issued to ensure the users that behind the website there is a legal person identifiable by trustworthy information.

- ***Legal effects**: The Regulation distinguishes between electronic signatures (8), advanced electronic signatures (9) and qualified electronic signatures (10), maintaining the principle that an electronic signature, shall be admissible as evidence in legal proceedings. It specifically provides that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the fact that it is in electronic form and also that a qualified electronic signature shall have the equivalent legal effect of a handwritten signature. It is also noted that a qualified electronic signature based on a qualified certificate issued in Greece (or in anyone Member State) shall be recognised as a qualified electronic signature in all other Member States. The same as above principle broadly applies vis-à-vis electronic seals, electronic time stamps, data sent and received using an electronic registered delivery service and electronic documents (11).*

- ***The Regulator**: In Greece the Hellenic Telecommunications & Post Commission ("EETT"), an Independent Administrative Authority, maintains the Registry (12), which includes information related to the qualified eTS providers for which it is responsible, together with information related to the qualified trust services provided by them.*

authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued.

(8) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

(9) 'advanced electronic signature' means an electronic signature which meets following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

(10) 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

(11) 'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording.

(12)http://www.eett.gr/opencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatures/EsignProviders.html

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

LEXING NETWORK

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons	John Giles	+27 (0) 21 300 1070	john@michalsons.com
Allemagne *Germany*	Beiten Burkhardt	Andreas Lober	+49 69 756095-0	andreas.lober@bblaw.com
Australie *Australia*	Madgwicks Lawyers	Dudley Kneller	+61 3 9242 4744	dudley.kneller@madgwicks.com.au
Belgique *Belgium*	Lexing Belgium	Jean-François Henrotte	+32 4 229 20 10	jf.henrotte@lexing.be
Brésil *Brazil*	Melchior, Micheletti e Amendoeira Advogados	Silvia Regina Barbuy Melchior	+ 55 113 8451511	melchior@mmalaw.com.br
Canada *Canada*	Langlois avocats, S.E.N.C.R.L.	Jean-François De Rico	+1 (418) 650 7000	jean-francois.derico@langlois.ca
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	jun.yang@jadefountain.com
Costa Rica *Costa Rica*	Lexing Costa Rica	Gabriel Lizama	+506 2253-1726	glizama@lexing.legal
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	marc.gallardo@lexing.es
États-Unis *USA*	Greenberg Traurig	Françoise Gilbert	+1 650-804 1235	gilbertf@gtlaw.com
France *France*	Alain Bensoussan Avocats Lexing	Alain Bensoussan	+33 1 82 73 05 05	paris@lexing.law
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	central@balpel.gr
Guatemala *Guatemala*	Morales, Redondo & Vargas	Ada Lissette Redondo Aguilera	+(502)2331-8057	aredondo@consejeros-legales.com
Inde *India*	Poovayya and Co	Siddhartha George	+91 80 4115 6777	siddhartha@poovayya.net
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	r.zallone@studiozallone.it
Japon *Japan*	Hayabusa Asuka Law Office	Koki Tada	+81 3 3595 7070	koki.tada@halaw.jp
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	info@kouatlylaw.com
Maroc *Morocco*	Fayçal Elkhatib et Associés S.C.P.A	Hatim Elkhatib	+212 5 39 94 05 25	hatim.elkhatib@elkhatiblawfirm.ma
Mexique *Mexico*	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De Gonzälez Argüelles	+ 52 55 25 91 1070	eochoa@carpio.law
Norvège *Norway*	Advokatfirmaet Føyen Torkildsen AS	Arve Føyen	+47 21 93 10 00	af@foyentorkildsen.no
Nouvelle-Calédonie *New Caledonia*	Cabinet Franck Royanez	Franck Royanez	+ 687 24 24 48	fr.avocat@cabinetroyanez.com
Portugal *Portugal*	Alves Pereira & Teixeira de Sousa	João P. Alves Pereira	+ 351 21 370 01 90	jpereira@alvespereira.com
Royaume-Uni *United Kingdom*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	dpreiskel@preiskel.com
Russie *Russia*	ALRUD	Maria Ostashenko	+ +7 495 234 96 92	mostashenko@alrud.com
Sénégal *Senegal*	SCP Faye & Diallo	Cheikh Faye Mamadou Seye	:(+221) 33 823 60 60	fayetdiallo@orange.sn seyemamadou9@gmail.com
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	sebastien.fanti@sebastienfanti.ch
Tunisie *Tunisia*	Younsi & Younsi International Law Firm	Yassine Younsi	+216 98 37 37 28	yassine.younsi@younsilawyers.com

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan
Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier
Diffusée uniquement par voie électronique – gratuit –
ISSN 1634-0701
Abonnement à partir du site : https://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-debat/