



---

SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE

---

**SIGNATURE ET CERTIFICATION ELECTRONIQUES  
ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE  
ELECTRONIC SIGNATURE AND CERTIFICATION  
BETWEEN LEGAL RELIABILITY AND AUTHENTICITY**

**ZAHDOUR Indjé-Hind Najoua Rime Soundous\***

Faculté de droit et sciences politiques ,Université  
d'Oran2 Mohamed BEN AHMED

ihzahdour@yahoo.fr

Date de réception: 25/06/2022

Date d'acceptation: 07/08/2022

Date de publication: 15/09/2022

---

**Résumé:**

Dans le contexte de la révolution électronique et des développements radicaux qui l'accompagnent sur la base desquels un acte juridique est conclu, La législation internationale et algérienne a vu la nécessité d'adopter un système formel de signature et de certification électroniques après avoir été gelé pendant des années.

Ce système a apporté une souplesse aux des transactions électroniques, quelle que soit le domaine de ces transactions, tout en renforçant le contrôle électronique pour assurer la confidentialité et la crédibilité des informations et des données incluses.

Pour refléter ce contrôle, des organes ad hoc ont été créés pour conférer authenticité et crédibilité à la signature et à la certification électroniques.

**Mots clés:** signature, certificat, électronique, authenticité, force probante.

**Abstract:**

In the context of the electronic revolution and the radical developments that accompany it on the basis of which a legal act is concluded, International and Algerian legislation saw the need to adopt a formal system of electronic signature and certification after having been frozen for years.

This system has provided flexibility to electronic transactions, regardless of the domain of those transactions, while strengthening electronic control to ensure the confidentiality and credibility of the information and data included.

To reflect this control, ad hoc bodies have been created to give authenticity and credibility to electronic signature and certification.

**Keywords:** signature, certificate, electronic, authenticity, probative force.

**Introduction**

L'actuelle vague du développement technologique est devenue le nouveau pilier sur lequel s'appuie la plupart des entreprises, qu'elles soient nationales ou internationales. Bien que ce pilier prévoie l'effort humain et même le coût de la sous-traitance et de la progression vers celui-ci, cet aspect positif peut être attiré par un sérieux inconvénient, qui est vulnérable au piratage et à la création de clients virtuels qui peuvent exposer ces actes à des crimes graves.

Le fait que les conseils de passation de marchés – qui sont censés être efficaces et valides - ne rencontrent pas physiquement les entrepreneurs et ont à traiter dans un environnement virtuel ouvert, a exposé les entrepreneurs et leur entreprise à

---

\*Auteur correspondant



---

**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

---

plusieurs risques qui peuvent entraîner le vol de leur identité ou le piratage de leurs comptes bancaires par des opérations de cyber piratage.

Le développement technologique a réduit les barrières du temps et de la distance, qui restent toutes dans le monde "traditionnel réaliste", de sorte que la législation a jugé nécessaire de revenir à des faits hypothétiques dans l'achèvement de la conduite contractuelle, dont la plupart comprenaient la procédure de signature électronique et les actes électroniques.

Ces procédures n'étaient pas facilement acceptables au début de leur apparition, d'autant plus que les contractants ne connaissaient que la signature écrite, qui était devenue selon les termes des juristes - traditionnelle, et ne traitait que des actes officiels sur support papier. Cela a conduit à la nécessité de modifier les lois sur la validité des procédures de passation des marchés, à laquelle le législateur algérien a répondu en adoptant ce système électronique en promulguant la loi 15-04 du 10/02/2015 sur la certification et la signature électroniques. Cela ne veut pas dire que cette disposition est la première à se rapporter aux transactions électroniques, mais elle a été précédée par d'autres dispositions, dont les plus importantes sont contenues dans la modification du Code civil en vertu de la Loi no 05-10 du 20/06/2005 modifiant le Code civil et les autres dispositions réglementaires contenues dans le présent document.

Face aux risques probables de ces dispositions virtuelles, il était nécessaire de créer des mécanismes et des technologies modernes qui suivent le rythme de la mondialisation afin de créer une source de confiance, de sécurité dans les transactions électroniques grâce au mécanisme de certification ou de documentation électronique. Cependant, malgré l'évolution de cette technologie, elle présente des inconvénients qui peuvent être également améliorées suite à sa mauvaise utilisation d'où peut se développer des responsabilités.

Compte tenu des préoccupations concernant la réticence de certains contractants, de la confiance et de la bonne utilisation de ces moyens développés par d'autres, la question qui peut se poser quant à la légalité du système de signature électronique et si les dispositions réglementaires et législatives peuvent protéger le signataire contre le risque d'utilisation abusive de cette procédure?

Pour tenter de répondre à cette problématique, ce travail sera traité comme suit:

I. Développement juridique des technologies de signature électronique et de certification

1- Concept moderne de la signature en vertu de la loi no 15-04

2- Importance juridique et pratique de la procédure de certification électronique

II. Force probante de la signature électronique et la certification et leur authenticité



---

SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE

---

- 1- Reconnaissance de l'authenticité complète de la signature électronique
- 2- Certification électronique et responsabilités des prestataires de service de certification électronique

### **CHAPITRE 1 : Développement juridique des techniques de signature électronique et de certification**

Il est bien établi dans la législation et la jurisprudence que l'écriture est non seulement un argument, mais aussi une expression de la volonté du signataire d'adhérer et d'approuver le contenu du document comme un moyen de distinguer l'identité du signataire<sup>1</sup>.

Une signature est un élément nécessaire à l'authenticité de la preuve écrite préparée - formellement ou habituellement - car la loi n'exige pas la signature en vain, mais plutôt parce qu'elle est un élément nécessaire de la force de la preuve écrite. Une signature n'est pas un élément de preuve écrit, mais plutôt une preuve pré-préparée de la présence obligatoire des parties pour agir et exprimer la volonté du signataire d'être lié par le contenu et l'approbation de l'acte<sup>2</sup>.

Face à la prolifération du système de traitement électronique de l'information, qui a commencé à envahir les entreprises, les départements et les banques, les procédures manuelles sont devenues non pertinentes et la signature manuelle est devenue un obstacle difficile à adapter aux systèmes modernes de gestion et de comptabilité<sup>3</sup>.

Pour qu'une signature électronique ait le pouvoir de prouver, elle doit remplir certaines conditions qui la renforcent et établissent les éléments de confiance et de sécurité<sup>4</sup>. Ces conditions comprennent la nécessité de la ratification. Le législateur algérien a promulgué la loi n° 05/10 modifiant et complétant le Code civil<sup>5</sup> par les dispositions des articles 323 bis et 327, qui ont donné à la signature écrite et électronique le même pouvoir de la preuve écrite. Le décret exécutif no. 07/162 du 30/05/2007 sur le système d'exploitation applicable à chaque type de réseau et à divers services de télécommunication a également abordé la signature électronique et la certification comme garantie de l'intégrité des transactions commerciales.

Le 01/02/2015, le législateur algérien a promulgué la loi n° 15/04<sup>6</sup>, qui énonce les dispositions relatives à la signature électronique et à la ratification.

#### **Premièrement : Concept moderne de la signature en vertu de la loi 15/04**

Le législateur a fait de la signature une condition essentielle et juridiquement indispensable à l'authenticité de la preuve écrite, qu'elle soit authentique ou sous seing privé. Une signature est la condition préalable à la validité de l'acte usuel préparé pour la preuve, car le document signé électroniquement contient un écrit prouvant ce qui a été convenu.



---

SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE

---

Quant au document authentique, en plus de la signature, il doit être délivré par un officier public ou une personne responsable d'un service public. Si la signature échoue, le document écrit perd l'exigence de fond qu'il soit considéré comme une preuve écrite<sup>7</sup>.

### **1. Notion de la signature traditionnelle**

La signature juridique est le résultat de l'expansion des relations commerciales et civiles entre les différentes sociétés en raison de l'évolution des modes d'écriture et de gouvernance, ainsi que du besoin de documentation d'identité. La jurisprudence internationale a défini la signature comme une «paraphe» et une «marque», ce qui permet de détecter et d'identifier facilement la personnalité du signataire, ou une empreinte sur le document pour exprimer son consentement juridique et son engagement<sup>8</sup>.

S'agissant d'abord de son contenu, la signature doit permettre d'identifier celui qui l'a apposé. C'est la raison pour laquelle elle doit en principe reproduire son nom et son prénom et être lisible. L'indication du seul patronyme- nom et prénom-peut suffire, même si ce n'est pas la manière habituelle de signer de celui qui les inscrit, dès l'instant cela est parfaitement de nature à l'identifier et à manifester son approbation<sup>9</sup>.

En revanche, on enseigne que la signature ne peut être constituée seulement d'initiales- les quelles constituent simplement un «paraphe»- car celles-ci, communes à une pluralité de personnes, ne permettent pas réellement d'identifier celui qui les a apposé<sup>10</sup>.

En général, la définition de la signature doit reposer sur deux aspects. Premièrement, la dimension fonctionnelle de la signature est définie, c'est-à-dire la définition des fonctions de la signature et, deuxièmement, l'identification de ses formes, en particulier avec l'émergence d'une signature électronique comme forme moderne de la signature<sup>11</sup>.

### **2. Définition de la signature électronique**

Une signature électronique, comme une signature traditionnelle, remplit diverses fonctions, y compris celle de preuve. Elle distingue également la personnalité du propriétaire et l'identifie, mais la signature électronique dépasse la signature traditionnelle en ce sens que l'identité du propriétaire peut normalement être vérifiée chaque fois que le NIP<sup>12</sup> du propriétaire est utilisé, et ce NIP est la signature électronique<sup>13</sup>.

En ce qui concerne la législation, la loi type de la CNUDCI<sup>14</sup> de 1996 sur le commerce électronique et ses textes rigoureux montrent qu'elle n'a pas été soumise à la définition d'une signature électronique, mais seulement à son pouvoir de preuve associé à la réalisation d'une gamme de fonctions. mais compte tenu du



---

SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE

---

rôle que joue la signature électronique dans la promotion de la confiance et de la sécurité dans les transactions électroniques<sup>15</sup>, la loi type de la CNUDCI a élaboré une définition complète en vertu de l'article 2/a qui « Les données sous forme électronique incluses, ajoutées ou logiquement associées à un message de données peuvent être utilisées pour identifier l'emplacement du message de données et pour indiquer l'approbation de l'emplacement de l'information contenue dans le message de données. »

L'Union européenne a été l'une des premières à préconiser l'adoption de la signature électronique comme signature conventionnelle et pour en faire un moyen de preuve acceptable<sup>16</sup>.

L'Union européenne a distingué deux types de signature électronique, la première étant une signature électronique simple ou ordinaire définie à l'article II comme "information sous forme électronique associée ou logiquement associée à d'autres données électroniques qui constituent la base de la méthode d'authentification". Cette définition identifie les moyens légaux par lesquels une signature électronique est faite sans indiquer les fonctions juridiques visées<sup>17</sup>.

Le deuxième type de signature électronique est une signature antérieure, avancée ou améliorée. Ce type de signature est défini par l'article II, paragraphe II, de la directive européenne comme une signature qui remplit les conditions suivantes:

- La signature doit appartenir individuellement et personnellement au signataire
- L'identification de l'emplacement peut être renseignée
- La création de la signature doit être placée sous le contrôle du signataire
- La signature doit être liée aux données auxquelles elle est rattachée de manière à rendre détectable toute modification ultérieure des données<sup>18</sup>.

Il ressort de ce qui précède que la directive européenne exige que la validité d'une simple signature électronique soit effectuée de manière technique fiable. La signature électronique sécurisée est approuvée par une entité spécialisée chargée de vérifier l'identité et le ratio de signature du signataire, et ce type de signature a la pleine authenticité de la preuve qui correspond à la signature traditionnelle<sup>19</sup>.

L'Algérie n'a pas été isolée du développement des transactions électroniques, et la modification du Code civil en vertu de la loi no 05/10 a été la première réglementation juridique de la signature électronique, car l'article 327/2, tel que modifié par la loi, stipule que "La preuve écrite est considérée sous forme électronique, comme la preuve écrite sur papier, à condition que l'identité de la personne qui la délivre puisse être vérifiée et soit préparée et conservée dans des conditions qui garantissent son intégrité."



---

**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

---

Cependant, en raison de l'importance de la signature électronique dans les transactions électroniques et de l'ouverture de l'économie nationale, la législation algérienne a dû créer une politique juridique qui fait face à de profonds changements tant dans les transactions économiques que dans les systèmes modernes de négociation. Le système juridique, qui ne répondait pas aux exigences de l'économie libre et n'est pas conforme à l'âge de la technologie, a adopté une loi spéciale n° 15/04 du 01/02/2015, qui établit les règles régissant la signature électronique et la certification<sup>20</sup>.

L'article 2 de la loi 15/04 stipule qu'une signature électronique est "...des données sous forme électronique, accompagnées ou logiquement liées à d'autres données électroniques, utilisées comme moyen de documentation".

Les données désignent les symboles ou les clés de chiffrement spéciales utilisés par le site pour créer la signature électronique "

Il convient de noter que la plupart des lois utilisent le terme « signature électronique » ou « signature » sous forme électronique en raison de l'absence d'accord sur une définition unique. Il s'agit d'une vision du développement rapide des moyens de communication et de l'émergence de nombreux types de signatures électroniques dans la pratique, ce qui conduira à l'élaboration de définitions<sup>21</sup>.

### **3. Formes de la signature électronique**

Comme d'autres législations nationales, la législation algérienne a distingué deux types de signatures électroniques, à savoir une signature électronique simple et sécurisée. Le premier type repose sur une gamme de moyens et de techniques qui atteignent le plus haut degré de sécurité et de confiance et empêchent la manipulation et l'altération<sup>22</sup>.

#### **a. Signature au stylo électronique**

Cette méthode permet au client ou à l'expéditeur de message de poser sa signature personnelle en utilisant un stylo électronique spécial sur l'écran de l'ordinateur et à travers un programme spécial. La signature est validée sur la base de mouvement de ce stylo et les formes qu'il prend, des cercles, courbes, et autres caractéristiques de signature de l'ordinateur du site, qui peut avoir déjà été stocké dans l'ordinateur et la signature dans le stylo électronique nécessite un ordinateur avec des spécifications spéciales qui lui permet d'effectuer sa tâche de capturer la signature de son écran et de vérifier sa conformité avec la signature mémorable dont il faut un authentifiant supplémentaire<sup>23</sup>.

Bien que cette forme de signature soit positive sur le plan de la flexibilité et de la facilité du transfert électronique manuel de la signature par les systèmes d'information, ce formulaire n'est pas très sécurisé car le destinataire peut



---

**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

---

conserver une copie de la photographie de signature et la relire à tout document électronique prétendant que l'auteur est le véritable signataire<sup>24</sup>.

**b. Signature numérique**

La signature numérique est l'une des images de signature électronique utilisées pour conclure une conduite légale au moyen de médias électroniques sur Internet. Cette image est basée sur l'utilisation de méthodes de cryptage qui sont techniquement une division de l'étude des mathématiques appliquées et intéressés à transformer le texte de son original, clairement lu forme en texte incompréhensible. Et ensuite restaurer ce texte à partir de sa forme originale, clairement lue en utilisant des équations mathématiques complexes appelées algorithmes de cryptage<sup>25</sup>.

**c. Signature codée**

Il est destiné à utiliser un ensemble de chiffres et de lettres ou les deux choisis par le signataire lui-même et utilisé pour signer la transaction électronique. Ce type est basé sur des cartes en plastique ou des cartes magnétiques avec mémoire électronique. Le titulaire de la carte l'insère correctement dans la machine de retrait et entre ensuite le PIN. En fin de compte, il presse le bon choix pour terminer le processus, et cette technologie facilite la conclusion des transactions commerciales et l'acquisition d'espèces à tout moment<sup>26</sup>.

**d. Signature biométrique**

Ce type de signature est basé sur les propriétés naturelles et chimiques des individus, il s'agit d'une application de types scientifiques appelés "biologie standard dans le domaine de la fibre", basée sur des mesures numériques des caractéristiques distinctives d'un être humain pour distinguer chacun des autres. Les systèmes d'information sont équipés de moyens biométriques qui permettent de stocker ces qualités sur l'ordinateur en prenant une photo, puis stockés numériquement dans la mémoire de l'ordinateur et cryptés de sorte que personne ne peut y accéder et essayer de les trafiquer<sup>27</sup>.

**Deuxièmement : Importance juridique et pratique de la procédure de certification électronique**

La signature électronique semblait confirmer l'identité des contractants et exprimer leur volonté de contracter et la plupart des lois ont limité la signature électronique à la validité de la preuve si certaines conditions sont remplies qui renforcent et donnent lieu à la confiance de telles conditions, La signature doit être ratifiée, ce qui nécessite qu'un tiers neutre confirme le consentement par le moyen d'un certificat contenant la signature électronique de la personne dont l'identité doit être établie<sup>28</sup>, et cette partie est appelée **Tiers de confiance**<sup>29</sup>

**1. Définition de la certification électronique**



---

**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

---

Les certificats électroniques sont des certificats délivrés par le prestataire de services autorisé ou certifié, qui montrent que la signature électronique est valide et attribuable exclusivement au signataire et qu'elle satisfait aux exigences légales en tant que preuve fiable<sup>30</sup>.

La législation algérienne traite la certification électronique au titre III de la loi 04/15 sur la signature électronique et la certification. La certification ou l'authentification électronique est un moyen technique sécurisé de vérifier l'authenticité de la signature ou du signataire. L'authenticité d'une signature électronique est vérifiée au moyen d'un certificat de certification électronique.

L'article 02/7, de la Loi définit un certificat électronique comme "un document sous forme électronique qui établit le lien entre les données de vérification de signature électronique et le signataire".

L'article II de la Loi type sur les signatures de la CNUDCI définit un certificat de certification électronique comme "un message de données ou autre enregistrement confirmant le lien entre le signataire et les données de création de signature".

Il est noté par la définition de la CNUDCI qu'elle a obligé le Prestataire de services de certification électronique à fournir un service de certification minimum avec la possibilité de fournir d'autres services liés à la signature électronique. Ses activités subsidiaires, et la Loi type sur la signature électronique n'a pas fait de distinction entre les situations dans lesquelles un prestataire de services de certification électronique exerce des services de certification en tant qu'activité filiale, coutumière, accidentelle, directe ou indirecte ou par l'intermédiaire d'un sous-traitant et du terme "personne" au profit de personnes physiques et morales<sup>31</sup>.

La législation algérienne, par l'article 2/11 et 12, de la loi no 15/04, distingue deux types de signataires. Le premier est un tiers de confiance et n'est qu'une personne morale; il ne délivre que des certificats électroniques prescrits et uniquement à l'intention de ceux qui font partie de la Direction générale du gouvernement sans la participation du public, comme les ministères. Le second est une personne physique ou morale. Les certificats électroniques simples ou prescrits sont délivrés au public et sont contrôlés par l'autorité économique de la certification électronique<sup>32</sup>.

## **2. Autorités de certification électronique**

Donner authenticité à une signature électronique doit être atteint sans nier ni oublier ses émetteurs, malgré la protection technique fournie lors de la création de la signature électronique, mais elle est insuffisante pour être pénétrée par des pirates. Compte tenu de ce piratage, il est nécessaire de trouver un moyen efficace





---

**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

---

d'empêcher l'imitation d'une signature électronique connue sous le nom de système de certification électronique<sup>33</sup>.

Le législateur algérien a désigné l'autorité compétente pour délivrer le certificat de certification électronique et l'a désigné comme l'exécutant du service de certification électronique. L'exécutant du service de certification électronique ne peut pas effectuer son travail sur la base d'une licence accordée par l'autorité économique pour la certification électronique. Ils peuvent également enregistrer la délivrance de subventions pour l'annulation et la conservation de certificats électroniques. Ils sont également tenus de garder confidentielles les données et informations sur la certification électronique : ils appliquent les tarifs pour les services accordés et ne peuvent pas refuser de fournir des services sans une raison valable, en plus des autres tâches spécifiées par le législateur dans la loi 04/15 sur la signature électronique et la certification<sup>34</sup>.

**Chapitre2 : L'authenticité souhaitée de la signature électronique et de la certification**

La plupart des lois ont respecté les conditions à imposer aux signatures électroniques afin de devenir un outil de preuve dans les transactions électroniques et de reconnaître ainsi leur authenticité absolue.

La plus importante de ces législations est la directive européenne sur les signatures électroniques, qui stipule qu'une signature électronique est ce qui a été collecté et comprend plusieurs conditions, dont la plus importante est son affiliation unique avec le signataire, la capacité de la signature à identifier le signataire, à créer par des moyens sous le contrôle exclusif du signataire et à lier la signature aux données de manière à détecter toute modification des données.

La législation algérienne a même été attirée par la puissance de la circulation électronique mondiale et le développement de textes spéciaux sur la signature électronique en vertu de la loi n° 15-04 du 10/02/2015 sur la signature électronique et la certification, sans parler des conséquences de l'extrapolation du texte du Code civil modifié. Les dispositions des règles de preuve sur la validité des actes électroniques, de la signature électronique et de l'écriture électronique ont été abandonnées.

Tant que la procédure de certification électronique repose sur la sécurisation et la confirmation des données de l'utilisateur ou du signataire et de la validité de cette signature, l'obligation principale du service de certification électronique est essentiellement limitée à la présentation d'un certificat électronique à la personne concernée, dont le but est de remplir sa fonction de certification de la signature électronique, en reconnaissant ainsi le comportement conclu par le signataire. Ainsi, le certificat électronique confirme les données relatives à la vérification et à



---

SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE

---

l'identification du signataire. Afin de légaliser ce signataire électronique, ce certificat doit à son tour contenir des données spéciales et donc faire autorité.

**Premièrement : l'authenticité de la signature électronique**

Le commerce numérique (électronique) connaît une vague de développement spectaculaire, ce qui nécessite d'assurer la valeur juridique de ce type de transaction. Cela ne peut être démontré qu'en consacrant une valeur juridique efficace et une authenticité à la signature et à l'écriture électroniques<sup>35</sup>.

Les tentatives des chercheurs sur l'authenticité d'une signature électronique et sa jouissance de l'authenticité absolue ont varié. Certains juristes estiment qu'il est nécessaire de donner une authenticité absolue à une signature électronique et d'autres ne reconnaissent même pas l'authenticité relative d'une telle signature. C'est principalement l'absence de l'idée de sécurité juridique à trouver dans ce type de signature<sup>36</sup>.

Toutefois, la promulgation de la loi type 2001 de la CNUDCI et les lois spéciales sur la signature électronique et le commerce lui ont fourni, à lui et à ses signataires, une protection juridique grâce à la validation des signatures par une entité autorisée qui émet des certificats<sup>37</sup>.

Pour que cette introduction soit plus convaincante pour ceux qui s'intéressent à l'authenticité d'une signature électronique, il serait acceptable d'étudier cette authenticité à trois égards : l'authenticité d'une signature électronique conformément à la loi type de la CNUDCI sur la signature électronique, l'avis de l'Union européenne sur la signature électronique et, enfin, l'authenticité d'une signature électronique dans les lois arabes.

**1. Force probante de la signature électronique en vertu de la Loi type de la CNUDCI**

Le contenu de l'article I de la Loi type de la CNUDCI est inévitable et sans équivoque, mais elle affirme que la loi a remplacé l'étude par l'établissement d'une règle impérative qui confirme et incarne l'introduction d'une signature électronique lorsqu'elle est utilisée dans des activités commerciales et que, à l'inverse, il n'abroge aucune disposition juridique qui assurerait la protection des contractants signataires.

La loi type de la CNUDCI adoptée par la Commission des Nations Unies en 2001 (précédée par la loi type de la CNUDCI sur le commerce électronique en 1996), tous deux visant à éliminer les obstacles juridiques à l'utilisation d'alternatives aux formes de communication sur support papier, en stockant les données dans l'achèvement des transactions et les preuves, et des règles uniformes sur les signatures électroniques. Dans son intégralité, la loi a affirmé son champ d'application qui rend ses dispositions applicables si des signatures électroniques



---

**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

---

étaient utilisées dans des activités commerciales. Elle ne limitait pas son champ d'application à l'utilisation de signatures électroniques en dehors du domaine commercial<sup>38</sup>.

La loi type prévoyait un principe important centré principalement sur l'authenticité d'une signature électronique en preuve et son lien avec la nécessité de limiter les conditions spécifiques à l'association de la signature avec son signataire et au système de signature contrôle exclusif du signataire, avec la possibilité de détecter tout changement qui pourrait se produire dans une signature électronique après son achèvement<sup>39</sup>.

Ainsi, toute personne ne peut prouver l'authenticité d'une signature électronique comme moyen d'établir la confiance dans les transactions signées, et le contraire peut être démontré par toute preuve possible<sup>40</sup>.

Pour qu'une signature électronique soit fiable du point de vue de son authenticité, elle doit être proportionnelle aux normes internationales reconnues, qui sont fondées sur la disponibilité des quatre dispositions mentionnées à l'article VI de la Loi type mentionnée précédemment. Pour que ces clauses se concrétisent, un ensemble d'obligations associées au processus de signature électronique incombent à la fois au signataire (article 8 de la Loi type sur la signature électronique) et au fournisseur de services d'authentification électronique (article 9 de la loi type sur la signature électronique). Chacune de ces parties doit s'engager à un certain degré de responsabilité afin d'assurer la sécurité, la confiance dans les transactions et la signature électronique.

De ce qui précède, le contenu des textes de loi de la CNUDCI qui ont repris la déclaration faisant autorité de la signature numérique (électronique) protégée semble avoir assimilé ce type de signature à l'écrit faisant autorité, signature écrite ou traditionnelle pourvu que certaines exigences soient respectées. Il semble à travers cela, et à travers les textes de législation comparée, qu'il n'est plus nécessaire de parler d'accords régissant l'authenticité de la signature électronique en preuve et il n'y a pas de place pour la controverse parmi les chercheurs sur la gravité de son authenticité.

## **2. Avis de l'UE sur la crédibilité de la signature électronique**

La position de l'Union européenne sur la signature électronique et son recours à l'authenticité absolue était plus raisonnable en ce sens qu'elle a empêché la controverse entre l'authenticité d'une signature électronique ou non par la position adoptée par le Conseil européen. Elle s'est efforcée d'identifier les axes clés sur lesquels les États se coordonnent pour prévenir tout conflit ou toute obstruction qui détournerait et entraverait le commerce électronique<sup>41</sup>. Les implications juridiques de la délivrance d'une signature électronique ont été initialement exposées, et il a



---

SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE

---

ensuite été stipulé qu'une telle signature devrait être certifiée de manière à permettre la reconnaissance mutuelle entre les États membres. Il a également mis l'accent sur les spécifications et les caractéristiques de la documentation de signature électronique et, enfin, les responsabilités des prestataires de services de certification de la signature électronique<sup>42</sup>.

L'article 5/F1 de la directive stipule : "Les États membres doivent veiller à ce que les signatures électroniques avancées fondées sur un certificat qualifié, créé par un outil de création de signature sécurisé:

- 1- répond aux mêmes exigences juridiques qu'une signature écrite.
- 2- admissible comme preuve dans une procédure judiciaire.

Ainsi, en vertu de cette directive, les États membres de l'Union européenne placent une signature électronique dans la même position juridique qu'une signature écrite et sont utilisés comme outil de preuve devant les tribunaux.

Si elle indique quelque chose, elle indique le pouvoir juridique de la signature électronique, comme en témoigne son acceptation devant les tribunaux<sup>43</sup>.

En cas de comparaison entre les dispositions de la directive européenne et la loi type de la CNUDCI sur la signature électronique, la directive européenne vise à établir des règles juridiques générales qui reconnaissent la signature électronique et reconnaissent l'authenticité de la signature électronique en preuve. La directive européenne stipule qu'une signature électronique doit satisfaire aux exigences suivantes:

- 1- La signature est liée seulement au signataire
- 2- Permission de l'identification du signataire
- 3- Mettre la signature sous contrôle exclusif du signataire
- 4- La signature est liée aux données auxquelles elle est transmise de manière à permettre la divulgation de chaque modification ultérieure<sup>44</sup>.

Cela peut sembler être une répétition de ce qui a déjà été dit dans la loi de la CNUDCI, mais cela a été délibéré afin de démontrer la similitude entre les deux textes. Ainsi, le point de vue européen souligne qu'aucune valeur juridique ne devrait être retirée d'une signature électronique tant qu'elle est basée sur un certificat de certification électronique approuvé et qu'elle répond aux exigences et critères techniques. Ainsi, une signature électronique du point de vue de la directive européenne est un argument de preuve complet, comme une signature traditionnelle (écrite).

### **3. Vision des lois arabes pour l'authenticité de la signature électronique**

Contenu dans la loi jordanienne sur les transactions électroniques No. 85 de 2001 stipule que le registre électronique, le contrat électronique et la signature électronique sont tous des actes ou des transactions qui produisent les mêmes effets



---

**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

---

juridiques que les actes écrits et les signatures écrites traditionnelles. L'article 31 de la loi précitée dispose que, si le résultat de l'application des procédures documentaires utilisées est jugé approuvé, acceptable sur le plan commercial ou convenu entre les parties, la signature électronique est réputée authentifiée si elle est caractérisée comme:

- Se distingue par son association avec la personne en question
- Il suffit de présenter le propriétaire.
- Elle a été créée par des moyens propres à la personne et sous son contrôle
- A été lié au registre auquel il se rapporte de manière à ne pas permettre une modification de l'enregistrement après signature sans changement de signature.

En conséquence, le droit jordanien présuppose que la signature électronique authentifiée est imputable à son auteur et que sa délivrance constitue une preuve de son acceptation du signataire électronique<sup>45</sup>. En vertu de ces conditions, une signature électronique en droit jordanien est jugée être de force probante et égale à une signature traditionnelle.

En ce qui concerne la loi tunisienne, en vertu de la Loi tunisienne sur les échanges et le commerce électronique no 73 de 2000, la validité juridique des preuves de signatures électroniques et de liens électroniques a été établie en ce qui concerne l'authenticité des signatures traditionnelles et des éditions officielles. Ceci est subordonné à la validité de la réglementation prévue par la législation tunisienne, qui stipule que toute personne souhaitant soumettre un document électronique peut créer son approvisionnement électronique à travers un système fiable, dont les spécifications techniques sont adaptées par décision du ministre chargé des communications.<sup>46</sup>

La loi tunisienne a reconnu la force probante de l'acte électronique et de la signature en preuve. Affirmant l'égalité entre les transactions écrites et électroniques, il a ajouté une règle générale selon laquelle la conclusion de contrats électroniques s'applique au système des contrats écrits traditionnels en termes d'affirmation, d'acceptation et d'effet juridique, et leur applicabilité d'une manière qui n'est pas incompatible avec les dispositions de la présente loi.<sup>47</sup>

Compte tenu de la législature égyptienne, il a également accordé la même force de preuve que celle qui a été établie pour la signature sur support papier pour la signature électronique. Comme la législation arabe et internationale, l'acquisition de cette authenticité par la signature électronique est liée à la disponibilité de certaines conditions, à savoir, le seul lien de la signature électronique au signataire, le contrôle du signataire unique sur l'intermédiaire électronique et la possibilité de détecter toute modification ou altération des relevés électroniques de l'éditeur ou



---

SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE

---

de la signature, ainsi que l'exigence que certains contrôles techniques soient mis à la disposition du législateur.<sup>48</sup>

La loi égyptienne n. 15 de 2004 affirme que la signature électronique est nécessaire dans les transactions individuelles et est invoquée dans le commerce électronique et que la signature électronique dans le cadre du droit civil, les transactions commerciales et administratives font autorité si elles doivent être établies et conclues dans les conditions prévues par la loi<sup>49</sup>, qui sont les mêmes que celles mentionnées ci-dessus.

La législation algérienne a suivi la vague des développements électroniques et l'évolution de la loi n° 15/04 du 10/02/2015 sur la signature et la ratification électroniques. Il a reconnu la nécessité des transactions électroniques, y compris les signatures électroniques par extension. L'article 07 de cette loi affirme que la signature électronique décrite est la signature électronique dans laquelle les exigences suivantes sont remplies:

- 1- établir la signature sur la base d'un certificat de certification électronique prescrit
- 2- La signature doit être liée seulement au signataire
- 3- Activer l'identification du signataire
- 4- Être conçu par un mécanisme de création de signature électronique sécurisé
- 5- A générer par des moyens sous le contrôle exclusif du signataire
- 6- Soit liée à ses propres données, de sorte que les changements subséquents à ces données puissent être divulgués.

Elle affirme l'égalité de validité juridique à l'article 08 du même acte entre une signature électronique décrite et une signature écrite, qu'elle soit de personne physique ou morale, et lui confère une validité juridique effective en preuve devant les tribunaux. Dans le même ordre d'idées, la législation algérienne met l'accent sur l'utilisation des signatures électroniques, à condition que la personne qui les délivre puisse être identifiée, préparée et conservée dans des conditions garantissant leur sécurité<sup>50</sup>.

En résumé, il est clair que la plupart des législations arabes a affirmé et reconnu la légalité de la signature électronique en preuve et que cette signature est combinée avec les exigences de l'organisation de chaque législation à réglementer selon son système, mais tous restent inspirés par la Loi modèle de la CNUDCI.

**Deuxièmement : Certificat de certification électronique et responsabilité du prestataire de services de certification et du titulaire de certificat électronique**

Les tendances législatives qui ont fait en sorte que la signature électronique soit authentique ont imposé de nombreuses procédures qui favorisent la sécurité et la



---

SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE

---

confiance. La procédure la plus importante pour distinguer ce type de transaction est l'authentification ou la certification électronique, dont le but est de s'assurer que la signature électronique délivrée dans le cadre d'une conduite légitime ou d'une transaction commerciale a été effectuée par une personne précise. Il s'agit d'une procédure qui permet de suivre tout changement ou toute erreur qui s'est produit dans un document électronique après sa création en se fondant sur l'utilisation de moyens spéciaux d'identification, le chiffrement de symboles, de chiffres, de mots et la restauration inversée qui permettrait d'atteindre l'objectif souhaité<sup>51</sup>.

La plupart des études législatives en ligne suite à la révolution technologique, les lois sur le commerce électronique, les lois spéciales et la validité de la signature électronique ont confirmé la nécessité d'imposer et de fournir des méthodes sûres pour l'utilisation appropriée de la signature électronique et de la crédibilité. Pour cette raison, des autorités ont été créées appelées prestataire de services de certification et titulaire de certificat électronique, dont le rôle est de délivrer un certificat d'une autorité compétente qui authentifie et valide la délivrance de la signature électronique du signataire. La conséquence de cette ratification est d'assurer la sécurité juridique des transactions commerciales électroniques et de leurs signatures.

Il peut sembler être le premier regard sur les textes spécifiques de cette transaction, mais en fait il cache des responsabilités qui peuvent avoir un impact négatif sur les e-certificateurs et les prestataires de services en cas de manquement à leurs obligations.

### **1- Valeur juridique du certificat de certification électronique**

Afin d'encourager les transactions électroniques et d'instaurer la confiance à leur égard, la législation électronique a cherché à fournir des garanties solides sur la base desquelles la volonté, l'identification et le taux de signature des contractants sont déterminés. Ces garanties sont le fruit de la création d'un tiers impartial, crédible et accrédité dont la tâche consiste à certifier les signatures électroniques. La raison en est que l'espace pour ce type de signature est déterminé par une machine, l'ordinateur, qui rassemble les gens qui sont espacés, qui ne se réunissent pas dans un conseil réel<sup>52</sup>.

Tant que les réseaux internet sont considérés comme des espaces ouverts et exposés au piratage et à la contrefaçon par des cyber-pirates qui ont l'expérience de la manipulation d'œuvres électroniques, et que ces risques ou crimes ne peuvent être rencontrés comme un bien public, les États devaient envisager de créer une entité faisant autorité pour certifier une signature électronique afin de protéger les intérêts et les droits des particuliers et des institutions qui utilisent ces signatures.



---

**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

---

À cet égard, la Loi type sur la signature électronique de la CNUDCI autorise l'identification de l'authentifiant du signataire. L'article 07 de la présente loi prévoit que toute personne, organe ou autorité désignée par l'autorité compétente, qu'elle soit publique ou privée, peut identifier les signatures qui satisfont aux dispositions de l'article 06 de la présente loi. Toute décision prise en vertu du paragraphe 1 devrait également être conforme aux normes internationales reconnues.

Le présent article vise à assurer la sécurité et la prévisibilité lorsque les parties utilisent des techniques de signature électronique.

Compte tenu du fait que l'espace de signature électronique est de nature contractuelle internationale et que l'hypothèse présomptive du nombre et de l'identité des randoisseurs reste inconnue, face à ce danger, il est nécessaire de créer un système de validation et les individus restent absolument libres d'utiliser la technologie dans leurs transactions contractuelles sous le titre de fiabilité établi par la loi type. Les parties concernées peuvent prouver devant la juridiction ou le tribunal arbitral que le mode de signature qu'elles ont choisi répond aux exigences de l'article 6. Ainsi, une signature électronique reste fiable conformément à la loi type<sup>53</sup>.

La loi de la CNUDCI définit donc le certificat d'authentification comme "un message de données ou autre document confirmant le lien entre le signataire et les déclarations d'origine de la signature"<sup>54</sup>.

Pour sa part, le législateur algérien n'a pas élaboré de définition terminologique ou législative du terme "certification électronique" et l'a trouvé par la disposition de la loi n. 15/04, qui affirme qu'un certificat de certification électronique doit être disponible selon une exigence particulière, en se limitant principalement à la nécessité d'un certificat de certification délivré par un tiers crédible ou par un exécutant de services de certification électronique. Ce certificat n'est délivré qu'au signataire et comporte un ensemble de conditions telles que l'identification du tiers certifiant le nom ou l'alias du certificat, les données relatives à la vérification électronique des signatures, la sécurité ", en ce qui concerne le début et la fin de la validité du présent certificat ainsi que d'autres conditions qui servent la sécurité du signataire<sup>55</sup>.

Il est tiré de cet article que le certificat de certification électronique sert de garantie et de visa de sécurité délivré par une autorité compétente qui bénéficie de la validité et du crédit de la transaction électronique, tant en ce qui concerne l'authenticité des données qu'il contient qu'en ce qui concerne le contenu de la transaction et de ses parties.





---

SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE

---

En résumé, le certificat d'authentification électronique est un certificat reliant les données du signataire à sa signature en vérifiant son identité après avoir été soumis à des exigences particulières. Le présent certificat vise à confirmer la délivrance de la signature électronique de ceux qui lui sont attribués.

La position du législateur algérien est claire sur la valeur juridique d'un certificat de certification électronique article 323 bis et 323 bis 1 sur le statut d'égalité entre les actes électroniques et écrites en termes de valeur juridique de la preuve, peu importe les moyens qu'il contient. son identité ", à condition qu'elle comporte la possibilité de vérifier l'identité de sa source et qu'elle soit préparée et conservée dans des conditions garantissant son intégrité.

Par la loi no 15/04, le législateur a également énoncé sa reconnaissance et l'authenticité de la signature électronique si elle est conforme aux conditions qui y sont énoncées.

Ainsi, bien que la position du législateur algérien sur la valeur juridique du certificat de certification électronique ne soit pas claire, son approbation de la signature électronique et son octroi de la même authenticité que la signature écrite et sa reconnaissance le signataire électroniques, le certificat de certification électronique est également le signataire électronique sous réserve de sa conformité aux exigences et conditions particulières.

## **2- Responsabilités des certificateurs électroniques**

La protection des contractants, tant en vertu de règles générales que de règles spéciales, est le statut le plus important dans les relations contractuelles. Les textes juridiques ont donc imposé une protection spéciale aux signataires par voie électronique et ont créé des implications juridiques pour les certificateurs en cas de violation des obligations des contractants. Pour refléter cette responsabilité et cette protection, l'intervention du tiers neutre (fournisseur de services d'e-certification) était nécessaire pour renforcer la crédibilité du système d'authentification électronique et des transactions électroniques respectivement.

Le législateur algérien, à l'instar d'autres législations internationales, a donc imposé des obligations à ces organismes, à savoir la protection des informations personnelles des contractants et celles relatives à l'activité des prestataires de services de documentation. En cas de manquement, ils sont responsables, qu'ils soient civils, criminels ou administratifs.

En matière de responsabilité civile contractuelle et de défaut, la relation entre le signataire et le certificateur repose essentiellement sur un actif contractuel entraînant des obligations et des droits mutuels et tout manquement à l'exécution ou à la mise en œuvre d'une obligation contractuelle de manière erronée ou tardive, causant des dommages au signataire. Il en résulte inévitablement une



**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

responsabilité contractuelle des parties certificatrices à l'achèvement de leurs trois piliers.

Si le certificat de certification électronique contient des informations incorrectes et endommage le signataire, la responsabilité par défaut du certificateur électronique, qui oblige la partie causant le dommage (le certificateur) à compenser si l'erreur est intentionnelle ou non, comme le certificateur est tenu d'assurer la validité des informations établies dans le certificat de certification<sup>56</sup>.

La faute d'un certificateur électronique peut également adapter un contrevenant punissable aux dispositions du Code pénal, ce qui entraîne nécessairement une responsabilité pénale, qui est accompagnée d'une sanction après des éléments suffisants. Selon l'article 51 bis du Code pénal algérien : « À l'exception de l'État, des groupes locaux et des personnes morales de droit commun, une personne morale est partiellement responsable des infractions commises en son nom par ses organes ou représentants légitimes lorsque la loi le prévoit.

La responsabilité pénale de la personne concernée n'exclut pas la responsabilité de la personne physique en tant qu'acteur original ou en tant que complice des mêmes actes »

Compte tenu du maintien de ces responsabilités et des sanctions qui en découlent en termes généraux, le législateur algérien, par la loi n° 15/04, a estimé que les transactions électroniques et leurs auteurs devraient être assortis de sanctions pénales spéciales proportionnelles à la nature de l'erreur électronique commise et de faire en sorte que le service de certification électronique qui a délivré le certificat de certification; Responsable de tout préjudice causé à un organisme ou à une personne physique ou morale qui s'est prévalu de ce certificat si :

- 1- Validité de tous les renseignements contenus dans le certificat de certification électronique
- 2- Vérifier, au moment de l'attribution du certificat, que le signataire dans lequel il est identifié possède toutes les données de vérification de la signature électronique approuvant la signature.
- 3- S'assurer que les données de création de signature peuvent être utilisées et vérifiées<sup>57</sup>.

L'exécutant de ces services de certification peut également être exclu de toute responsabilité et, si de tels dommages sont indiqués dans le certificat de certification, la valeur maximale des transactions dans lesquelles le certificat peut être utilisé, à condition que cette référence soit vague<sup>58</sup>.



---

SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE

---

Le fournisseur peut également ne pas être tenu responsable si le titulaire du certificat ne respecte pas les exigences relatives à l'utilisation des données de signature électronique<sup>59</sup>.

D'autre part, le législateur a également tenu le titulaire du certificat responsable en tant que seul fonctionnaire du certificat dès qu'il a été signé et qu'il ne pouvait pas l'utiliser s'il expirait et ne l'utiliserait pas à des fins autres que celles pour lesquelles il a été délivré.

**Conclusion :**

Nous ne sommes pas libres de l'impératif d'entrer dans le monde virtuel, que ce soit une question ou une préférence. Cet accès peut être imposé par la législation internationale et nationale qui a diminué la volonté de l'entrepreneur par un simple click de bouton exprimant son acceptation et la conclusion des contrats, des transactions commerciales, civiles et même administratives; il s'est conclu par la signature de la récupération de la signature écrite du registre et a également fait la signature électronique sous forme de données, de codes et de chiffrements à inclure dans une base de données préservée de chaque entrepreneur.

Afin de garantir la légitimité de cette procédure, notre législation a réussi à assimiler la force juridique que les signatures traditionnelles ou les actes officiels peuvent obtenir aux signatures électroniques et aux signataires et à sécuriser les transactions dans ce contexte. Cette assurance est liée à la nécessité de respecter et de fournir des conditions techniques légales et des contrôles qui permettent la vérification, l'identification et la vérification de la volonté du signataire sur le contenu du contrat signé.

En réponse, la plupart des lois reconnaissent la force d'une telle signature tant qu'elle existait dans un cadre juridique rationnel et la rendaient admissible devant les tribunaux.

En ce qui concerne la crédibilité et la fiabilité de la signature électronique, la législation des États, y compris celle de l'Algérie, a estimé que les certificateurs devraient être soumis à des obligations, d'une part, et a obligé les signataires à faire preuve d'un soin et d'une discrétion suffisants pendant la signature. Cet objectif n'est atteint que par une procédure appelée certification électronique.

La procédure de certification électronique est un processus technique imposé par des circonstances obligatoires liées au commerce et à l'économie numériques. Le monde en ligne du Web a connu un développement radical dans les techniques de sécurité des transactions électroniques, ce qui a conduit les lois à se tenir au courant de cette vague, réglementer les questions de crédit et la confiance dans les transactions à travers les lignes et les fibres du Réseau.



---

**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

---

Malgré toutes les améliorations que ces transactions apportent et malgré tous les crédits et garanties fournis par le monde virtuel sous contrat électronique, la prudence et la vigilance restent nécessaires face aux risques de ces technologies développées

- <sup>1</sup> -Rachid BOUBEKEUR, « Signature électronique dans la législation algérienne (étude comparative) », Journal of Teacher Researcher of Legal and Political Studies, Université de M'sila, Vol 01, N°04, 2016, p.65. <https://www.asjp.cerist.dz/en/article/71391>
- <sup>2</sup> -Saadi El RABI, valeur probante de la signature électronique dans la législation algérienne, Thèse de Doctorat, Spécialité Droit pénal, Université de Batna, 2016, p.14.
- <sup>3</sup> -Ahmed BEN HAJA, « Authenticité juridique de la signature électronique dans la législation algérienne et droit comparé », Vol. 5, n° 2, 2016, p.297. <https://www.asjp.cerist.dz/en/article/30458>
- <sup>4</sup> -Kamel Fethi DRISS, "the Authentication Mechanism Of Electronic Security For Commercial Dealings With Modern Facilities In The Algerian Legislation", Journal of Studies and Research, El Oued University, Vol.14, n°2, 2017, p.160. <https://www.asjp.cerist.dz/en/article/27315>
- <sup>5</sup> -Loi n° 05/10 du 20/06/2005 modifiant et complétant l'ordonnance n° 75/58 du 26/09/1975 contenant le Code civil, Journal officiel n° 64 de 2005.
- <sup>6</sup> -Loi n° 15/04 du 01/02/2015, établissant les règles générales relatives à la signature et à la certification électronique, journal officiel, n° 06 de 2015.
- <sup>7</sup> - Saadi El RABI, op.cit., p.15.
- <sup>8</sup> - Ahmed BEN HAJA, op.cit., p.298.
- <sup>9</sup> - Cass.1<sup>er</sup> civ., 22 juin 2004 : Bull.civ.2004, 1, n°2953, note M.Nicod : « Attendu, cependant, que, même si elle ne constitue pas la signature habituelle du testateur, la mention de la main de celui-ci de ses nom, prénom au bas du testament répond aux exigences du texte susvisé(C. civ. Art.970)dès lors elle ne laisse aucun doute sur l'identité de l'auteur ni sur sa volonté d'en approuver les dispositions »
- <sup>10</sup> -Cass.com., 19 mai 1954 : Bull.civ.1954,3, n°187, -V.contra.CA Paris, 22 mai 1975 « En l'absence de toute définition légale de la signature, il y a lieu d'admettre que constitue une signature valable toute marque distinctive et personnelle manuscrite permettant d'identifier son auteur sans doute possible et traduisant la volonté non équivoque de celui-ci de consentir à l'acte, dès lors, un acte notarié constatant une donation peut être déclaré valable en la forme, bien que le donateur n'ait apposé à la fin de l'acte que ses initiales »
- <sup>11</sup> -Mohamed Réda AZRO, Conflits de preuve des contrats électroniques, Thèse de doctorat, Université de Tlemcen, 2016, p.167.
- <sup>12</sup> - NIP signifie Numéro d'Identification Personnel.
- <sup>13</sup> -Najia Badi BOUKMIJA, « Preuve du contrat électronique », Revue de Droit et sciences Humaines, Université Ziane Achour de Djelfa Vol. 10, n° 2, 2017, p.362. <https://www.asjp.cerist.dz/en/article/31429>
- <sup>14</sup> - **Commission des Nations unies pour le droit commercial international**  
La Commission des Nations unies pour le droit commercial international (CNUDCI) a été créée par l'Assemblée générale des Nations unies par sa résolution 2205 du 7 décembre 1966 pour promouvoir l'harmonisation et l'unification progressives du droit commercial international.  
La CNUDCI effectue son travail lors des sessions annuelles tenues alternativement à New York et Vienne. Principal organe juridique du système des Nations Unies dans le domaine du droit commercial international. Organe juridique à participation universelle spécialisé dans la réforme du droit commercial dans le monde depuis plus de 50 ans, la CNUDCI s'attache à moderniser et à harmoniser les règles du commerce international.



**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

- <sup>15</sup> -Mounira ABIZA, « La signature électronique garantie juridique pour la protection des consommateurs électroniques », revue académique des recherches juridiques et politiques, Université Omar Telidji de Laghouat Vol1, n°3, 2018, p.182. <https://www.asjp.cerist.dz/en/article/70372>
- <sup>16</sup> - Mohamed Réda AZRO, op.cit., p. 189.
- <sup>17</sup> - Saadi El RABI, op.cit., p.41.
- <sup>18</sup> -Saadi El RABI, ibid., p. 42.
- <sup>19</sup> - Mounira ABIZA, op.cit., p. 184.
- <sup>20</sup> - Saadi El RABI, ibid., p. 43.
- <sup>21</sup> -Mohamed Réda AZRO, op.cit., p. 197.
- <sup>22</sup> - Mounira ABIZA, op.cit., p. 187.
- <sup>23</sup> - Rachid BOUBEKEUR, op.cit., p.70.
- <sup>24</sup> - Rachid BOUBEKEUR, ibid., p.71.
- <sup>25</sup> - Saadi El RABI, op.cit., p. 57.
- <sup>26</sup> - Saadi El RABI, op.cit., p. 57.
- <sup>27</sup> - Mohamed Réda AZRO, op.cit., p. 214.
- <sup>28</sup> -Moustapha SAHRAOUI, « Protection technique et pénale de la signature en vue de la loi 15/04 sur la signature électronique et la certification », Journal of Research in Law and Political Science, Université Ibn Khaldoun de Tiaret, Vol 4, n°2, 2018, p.98. <https://www.asjp.cerist.dz/en/article/67529>
- <sup>29</sup> - Article 2 /11 de la loi 15-04. Tiers de confiance : personne morale qui délivre des certificats électroniques qualifiés ou éventuellement fournit d'autres services en matière de certification électronique au profit des intervenants dans la branche gouvernementale.
- <sup>30</sup> -Saadi El RABI, op.cit., p. 290.art.2/12 de la loi 15-04 : Prestataire de services de certification électronique : personne physique ou morale qui délivre des certificats électroniques qualifiés et fournissant éventuellement d'autres services en matière de certification électronique.
- <sup>31</sup> - Saadi El RABI, op.cit., p. 114.
- <sup>32</sup> -Redouane KERWECHÉ, « Organismes de certification électronique en vertu de la loi 15/04 sur les règles générales de signature et de certification électronique Concept et obligations », Revue des sciences sociales, Université de Sétif 2, Vol.14, n°1, 2017, p.413. <https://www.asjp.cerist.dz/en/article/30143>
- <sup>33</sup> -Aziza LARGAT, « Protection pénale de la signature électronique et la certification », Université de Tamenghasset, Vol.6, n°1, 2017, p.110. <https://www.asjp.cerist.dz/en/article/9138>
- <sup>34</sup> - Najia Badi BOUKMIJA, op.cit., p.370.
- <sup>35</sup> - Omar Ahmed LARAYCHI, Authenticity of Electronic Bonds in Proof, Al Hamid Publishing and Distribution House, Jordan, First Edition 2016, p. 101.
- <sup>36</sup> - Laurens ABIDET, Proof of Electronic Editor, Culture Publishing and Distribution House, Amman Jordan, 2005, p. 156.
- <sup>37</sup> - Dezza YII AZAD, « Système juridique de certification de la signature électronique en Irak : une étude comparative », Centre national de recherche, Palestine, Vol3, n°5, p. 80.
- <sup>38</sup> - Dezza YII AZAD, Ibid, p.85.
- <sup>39</sup> - Article 6 de la loi type de 2001 sur les signatures électroniques.
- <sup>40</sup> -Abdel Fattah Bayoumi Hijazi, Electronic Signature in Comparative Legal Systems, University Think edition, Egypt, 2004, p. 270.
- <sup>41</sup> - Article 34 de la directive européenne sur les signatures électroniques pour 1999.
- <sup>42</sup> -Hamid Suleyman DADYARE, Rôle des obligations en ligne pour preuve des affaires civiles, étude analytique comparative, thèse de Magister, Iraq, 2005, 173.
- <sup>43</sup> -Mohamed Mohamed Sadat, Force probante des actes signés électroniquement en preuve, étude comparative, New University House, Egypte, 2015, p. 144.



**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

- <sup>44</sup> - Article 3 de la directive européenne 13/12/1999 sur les signatures électroniques.  
<sup>45</sup> - Mohamed Mohamed Sadat, op.cit., p.148.  
<sup>46</sup> - Article 05 de la loi tunisienne sur le commerce et le commerce électronique no 73 de 2000.  
<sup>47</sup> - Chapitre I/paragraphe 2 de la loi n° 73 de 2000 de la Tunisie.  
<sup>48</sup> - Mohsen Abd al-Hamid Ibrahim AL-BAYH, Role of Electronic Editors in Evidence in Egyptian Law, reference inedited, p. 114.  
<sup>49</sup> - Article 14 d e la Loi égyptienne sur les signatures électroniques n° 15, 2004.  
<sup>50</sup> - Articles 323 bis 1 et 327 du code civil algérien.  
<sup>51</sup> - Omar Ahmed LARAYCHI, op.cit, p. 103.  
<sup>52</sup> - Ibrahim al-Dosouki ABU AL-LIL, Aspects juridiques des transactions électroniques, Conseil de l'édition scientifique, Université du Koweït, 2003, p. 177.  
<sup>53</sup> - Dezza YII AZAD, op.cit, p. 109.  
<sup>54</sup> - Article 2/b de la loi type de la CNUDCI sur les signatures électroniques.  
<sup>55</sup> - Article 15 de la loi n° 15/04 du 10/02/2015 sur la certification et la signature électroniques, Journal officiel n° 06.  
<sup>56</sup> - Abdel Fattah Bayomi HIJAZI, Signature électronique dans les systèmes juridiques comparatifs, Université Dar al-fikr, Alexandrie, 2005, p. 190.  
<sup>57</sup> - Article 53 de la loi no 15/04 sur la signature et la certification électroniques.  
<sup>58</sup> - Article 56 de la loi no 15/04 sur la signature et la certification électroniques.  
<sup>59</sup> - Article 57 de la loi no 15/04 sur la signature et la certification électroniques.

**Bibliographie :**

**Premièrement: les textes juridiques**

- Loi n° 05/10 du 20/06/2005 modifiant et complétant l'ordonnance n° 75/58 du 26/09/1975 contenant le Code civil, Journal officiel n° 64 de 2005.
  - Loi n° 15/04 du 01/02/2015, établissant les règles générales relatives à la signature et à la certification électronique, journal officiel, n° 06 de 2015.

**Deuxièmement: ouvrages**

- Omar Ahmed LARAYCHI, Authenticity of Electronic Bonds in Proof, Al Hamid Publishing and Distribution House, Jordan, First Edition 2016
- Laurens ABIDET, Proof of Electronic Editor, Culture Publishing and Distribution House, Amman Jordan, 2005
- Abdel Fattah Bayoumi Hijazi, Electronic Signature in Comparative Legal Systems, University Think edition, Egypt, 2004
- Mohamed Mohamed Sadat, Force probante des actes signés électroniquement en preuve, étude comparative, New University House, Egypte, 2015
- Mohsen Abd al-Hamid Ibrahim AL-BAYH, Role of Electronic Editors in Evidence in Egyptian Law, reference inedited
- Ibrahim al-Dosouki ABU AL-LIL, Aspects juridiques des transactions électroniques, Conseil de l'édition scientifique, Université du Koweït, 2003
- Abdel Fattah Bayomi HIJAZI, Signature électronique dans les systèmes juridiques comparatifs, Université Dar al-fikr, Alexandrie, 2005

**Troisièmement: thèse et mémoires**

- Saadi El RABI, valeur probante de la signature électronique dans la législation algérienne, Thèse de Doctorat, Spécialité Droit pénal, Université de Batna, 2016.
- Mohamed Réda AZRO, Conflits de preuve des contrats électroniques, Thèse de doctorat, Université de Tlemcen, 2016.



---

**SIGNATURE ET CERTIFICATION ELECTRONIQUES ENTRE FIABILITE JURIDIQUE ET AUTHENTICITE**

---

- Hamid Suleyman DADYARE, Rôle des obligations en ligne pour preuve des affaires civiles, étude analytique comparative, thèse de Magister, Iraq, 2005.
- Quatrième: Articles**
- Rachid BOUBEKEUR, « Signature électronique dans la législation algérienne (étude comparative) », Journal of Teacher Researcher of Legal and Political Studies, Université de M'sila, Vol 01, N°04, 2016. <https://www.asjp.cerist.dz/en/article/71391>
- Saadi El RABI, valeur probante de la signature électronique dans la législation algérienne, Thèse de Doctorat, Spécialité Droit pénal, Université de Batna, 2016..
- Ahmed BEN HAJA, « Authenticité juridique de la signature électronique dans la législation algérienne et droit comparé », Vol. 5, n° 2, 2016. <https://www.asjp.cerist.dz/en/article/30458>
- Kamel Fethi DRISS, "the Authentication Mechanism Of Electronic Security For Commercial Dealings With Modern Facilities In The Algerian Legislation", Journal of Studies and Research, El Oued University, Vol.14, n°2, 2017. <https://www.asjp.cerist.dz/en/article/27315>
- Redouane KERWECH, « Organismes de certification électronique en vertu de la loi 15/04 sur les règles générales de signature et de certification électronique Concept et obligations », Revue des sciences sociales, Université de Sétif 2, Vol.14, n°1, 2017. <https://www.asjp.cerist.dz/en/article/30143>
- Aziza LARGAT, « Protection pénale de la signature électronique et la certification », Université de Tamenghasset, Vol.6, n°1, 2017. <https://www.asjp.cerist.dz/en/article/9138>
- Mounira ABIZA, « La signature électronique garantie juridique pour la protection des consommateurs électroniques », revue académique des recherches juridiques et politiques, Université Omar Telidji de Laghouat Vol1, n°3, 2018. <https://www.asjp.cerist.dz/en/article/70372>
- Moustapha SAHRAOUI, « Protection technique et pénale de la signature en vue de la loi 15/04 sur la signature électronique et la certification », Journal of Research in Law and Political Science, Université Ibn Khaldoun de Tiaret, Vol 4, n°2, 2018. <https://www.asjp.cerist.dz/en/article/67529>
- Najia Badi BOUKMIJA, « Preuve du contrat électronique », Revue de Droit et sciences Humaines, Université Ziane Achour de Djelfa Vol. 10, n° 2, 2017. <https://www.asjp.cerist.dz/en/article/31429>
- Dezza YII AZAD, « Système juridique de certification de la signature électronique en Irak : une étude comparative », Centre national de recherche, Palestine, Vol3, n°5.