LES ENJEUX DE VALIDATION ET DE SECURITE DES DOCUMENTS NUMERIQUES : ZOOM SUR LA SIGNATURE ELECTRONIQUE AU MAROC

Safae Abrighach

▶ **To cite this version:**

Safae Abrighach. LES ENJEUX DE VALIDATION ET DE SECURITE DES DOCUMENTS NUMERIQUES : ZOOM SUR LA SIGNATURE ELECTRONIQUE AU MAROC. Revue Droit et Société ⊠⊠⊠⊠] ⊠⊠⊠⊠⊠⊠⊠ ,[⊠⊠⊠⊠⊠⊠⊠⊠⊠ 2023, 3 (9), pp.20- 30. ⟨10.5281/zenodo.7847614⟩. ⟨hal-04084238⟩

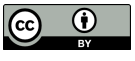
HAL Id: hal-04084238

https://hal.science/hal-04084238v1

Submitted on 27 Apr 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons CC BY 4.0 - Attribution - International License

REVUE
DROIT & SOCIETE
مجلة
القانون و المجتمع
دورية علمية محكمة تعنى با لدراسات و الأبحاث في المجال القانوني و الاجتماعي و الاقتصادي.
PERIODIQUE SCIENTIFIQUE A COMITE DE LECTURE, CONSACRE A LA PUBLICATION D'ETUDES
ET DE RECHERCHES DANS LES DOMAINES JURIDIQUE, ECONOMIQUE ET SOCIAL

LES ENJEUX DE VALIDATION ET DE SECURITE DES DOCUMENTS NUMERIQUES : ZOOM SUR LA SIGNATURE ELECTRONIQUE AU MAROC

THE STAKES OF VALIDATION AND SECURITY OF DIGITAL DOCUMENTS: FOCUS ON ELECTRONIC SIGNATURE IN MOROCCO

DOI: 10.5281/zenodo.7847614

Safae ABRIGHACH

Docteure en Droit Privé

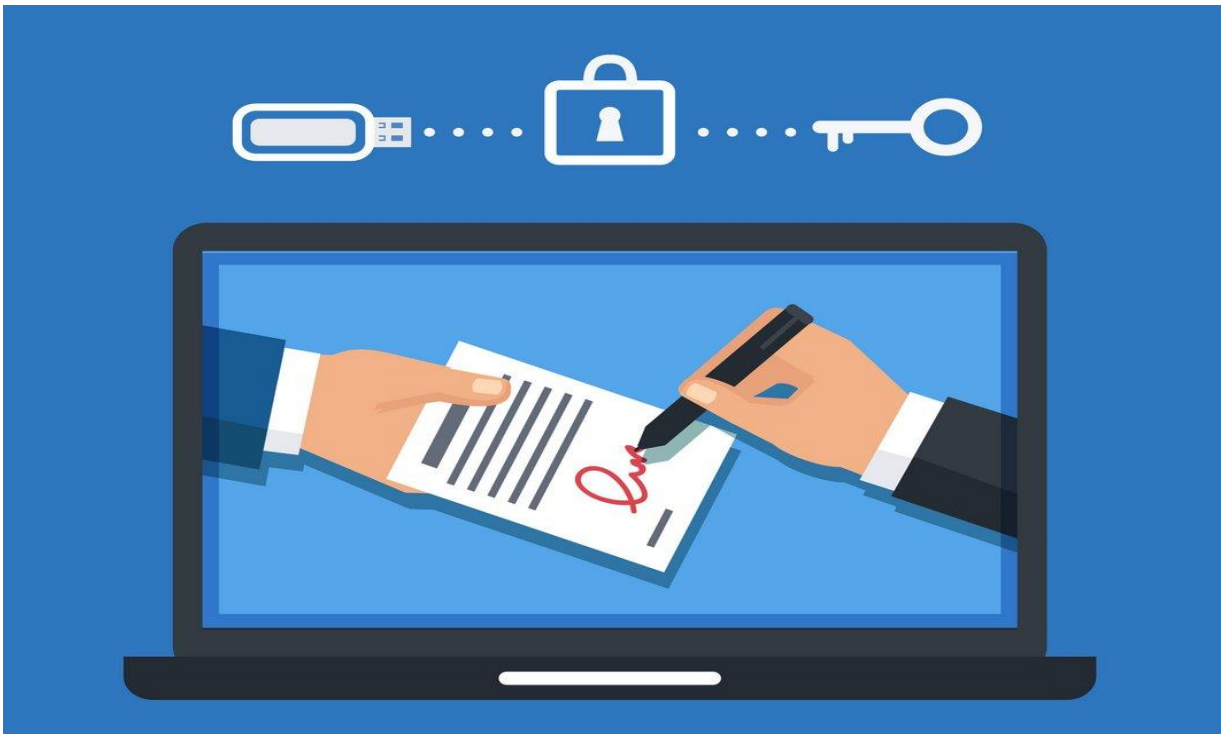
Université de Strasbourg, France

REVUE DROIT & SOCIETE
N° 9 – AVRIL / JUIN 2023

CC BY

Éditée Par
SOCIAL AND MEDIA STUDIES INSTITUTE
REVUE DROIT & SOCIÉTÉ
ISSN : 2737-8101

LES ENJEUX DE VALIDATION ET DE SECURITE DES DOCUMENTS NUMERIQUES : ZOOM SUR LA SIGNATURE ELECTRONIQUE AU MAROC



REVUE DROIT & SOCIETE
N° 9 – AVRIL / JUIN 2023

Safae ABRIGHACH

Docteure en Droit Privé

Université de Strasbourg, France

RESUME

Elément clé de la transformation numérique des entreprises et des services publics, la signature électronique contribue à l'efficacité, à la rapidité et à la sécurité des échanges et des transactions en ligne. En plus de pouvoir conclure des contrats à distance, elle permet de faciliter les échanges commerciaux et de réduire les coûts liés aux transactions papier. La signature électronique offre également des avantages en termes de traçabilité et de preuve juridique. Elle permet d'attester de l'identité du signataire, de la validité de son engagement et de la date et l'heure de la signature. Cette traçabilité facilite la résolution des litiges en cas de différends sur l'exécution d'un contrat.

Cet article a pour but d'étudier l'importance de la signature électronique au Maroc en termes de validation et de sécurité des documents numériques. Il convient d'examiner dans ce sens

les dispositions de la loi n°53-05 relative à l'échange électronique de données juridiques tout en se penchant sur les règles de la loi n°43-20 relative aux services de confiance pour les transactions électroniques

Mots clés : *Signature électronique, validation des documents numériques, sécurité des échanges électroniques, transformation numérique, preuve juridique des documents.*

THE STAKES OF VALIDATION AND SECURITY OF DIGITAL DOCUMENTS: FOCUS ON ELECTRONIC SIGNATURE IN MOROCCO

Safae ABRIGHACH

PhD in Private Law

University of Strasbourg, France

ABSTRACT

As a key element of the digital transformation of businesses and public services, electronic signature contributes to the efficiency, speed, and security of online exchanges and transactions. In addition to being able to conclude contracts remotely, it facilitates commercial exchanges and reduces costs related to paper transactions. Electronic signature also offers advantages in terms of traceability and legal evidence. It makes it possible to attest to the signer's identity, the validity of the signature, and the date and time of the signature. This traceability facilitates the resolution of disputes in case of disagreements over the execution of a contract.

This article aims to study the importance of electronic signature in Morocco in terms of validation and security of digital documents. In this regard, it is necessary to examine the provisions of Law No. 53-05 on electronic exchange of legal data while looking at the rules of Law No. 43-20 on trust services for electronic transactions.

Keywords: *Electronic signature, validation of digital documents, security of electronic exchanges, digital transformation, legal proof of digital documents*.

INTRODUCTION

Avec des avantages tels que la commodité, la sécurité et les économies de coûts, le contrat électronique est devenu un moyen courant de réaliser les différentes procédures et transactions numériques. Au Maroc, le contrat électronique est défini par l'article 2 de la loi n° 53-05 relative à l'échange électronique de données juridiques comme étant un contrat conclu par voie électronique, à distance, et qui utilise une méthode électronique pour son élaboration, sa conclusion ou sa communication. Il diffère du contrat informatique dans la mesure où ce dernier vise des dispositions spécifiques liées à l'utilisation de produits ou de services électroniques (*Huet*, 2021). Plus précisément, un contrat électronique est un contrat qui est conclu à travers l'utilisation d'un support électronique, tel qu'un site web, une application mobile, un courriel, ou tout autre moyen de communication électronique. Il doit être établi, signé et transmis par voie électronique (*Rahajaritsimba*, 2022).

En l'occurrence, pour qu'un contrat électronique soit valide et opposable aux parties, il doit respecter les mêmes conditions de validité que les contrats traditionnels. En se basant sur les dispositions de l'article 2 et suivant du Dahir formant Code des Obligations et des Contrats (DOC), cela signifie qu'il doit être librement consenti, avoir un objet licite et être conforme aux dispositions légales en vigueur. En ce sens, les parties doivent s'assurer que les conditions de formation du contrat sont respectées, notamment en ce qui concerne l'offre et l'acceptation[1]. Les parties doivent également conserver une trace de l'échange électronique, afin de pouvoir prouver la validité du contrat en cas de litige (*De Lamberterie*, 2006). Par conséquent, la loi marocaine relative à l'échange électronique de données juridiques fixe certaines exigences particulières en ce qui concerne la validité des signatures électroniques, la protection des données personnelles, la confidentialité des informations et la sécurité des échanges électroniques.

En droit marocain, la signature électronique est régie d'une part par la loi n° 53-05 relative à l'échange électronique de données juridiques et de l'autre par la loi 43-20 relative aux services de confiance pour les transactions électroniques. La signature électronique est définie comme étant l'ensemble des données électroniques qui accompagnent ou qui sont annexées à un message électronique et qui permettent d'identifier le signataire et d'exprimer son consentement. Une telle définition est large et inclut toutes les formes de signatures électroniques, des plus simples aux plus complexes. Dans la pratique, la signature électronique est largement utilisée dans les transactions numériques, notamment dans les secteurs de la finance, du commerce électronique et des contrats publics. Etant un outil important pour la numérisation des entreprises et la modernisation de l'administration publique, elle permet de faciliter les démarches en ligne, de réduire les délais de traitement et d'améliorer l'efficacité du service rendu (*Al-Rachadi*, 2022). Par ailleurs, la crise sanitaire de la Covid-19 a accéléré l'adoption de la signature électronique dans de nombreux domaines, en particulier dans le cadre de la signature de contrats à distance (*Ngombé*, 2022). Placée en tant qu'une alternative à la signature manuscrite, la signature électronique se distingue par certains avantages en matière de sécurité, de coût et de temps. En tant que procédé fiable d'identification, elle s'impose comme un outil de protection des données pour les parties signataires. L'idée est d'instaurer les conditions nécessaires pour assurer la confiance des acteurs de la société en l'économie numérique.

En considérant les éléments exposés précédemment, il est nécessaire de se poser la question suivante : Quel est le cadre juridique applicable à la signature électronique au Maroc ? L'intérêt d'étudier la réglementation de la signature électronique permet de comprendre les exigences légales mais aussi d'évaluer les risques juridiques. L'étude de la loi électronique permet également d'identifier les bonnes pratiques tout en contribuant au développement des politiques publiques.

En l'occurrence, la première partie de cette recherche portera sur l'analyse des législations en vigueur relatives à la signature électronique. La seconde partie, quant à elle, se concentrera sur la sécurité juridique et le contrôle des signatures électroniques.

I- La signature électronique comme mécanisme de validation des documents numériques

La loi 53-05 relative à l'échange électronique de données juridiques a été

[1] Chapitre premier Bis du Code des Obligations et des Contrats

adoptée au Maroc en 2007 pour encadrer l'utilisation de la signature électronique et des contrats électroniques. Inspirée de la loi type de la Commission des Nations Unies pour le droit commercial international (CNUDCI) sur l'e-commerce et sur la signature électronique (*Alassaire*, 2015), cette loi vise à instaurer la confiance dans les transactions électroniques en garantissant l'intégrité, l'authenticité et la confidentialité des échanges.

1/ Les critères de validation d'une signature électronique

La loi n°53-05 relative à l'échange électronique de données juridiques reconnaît la validité des contrats conclus par voie électronique au même titre que les contrats signés sur papier (*Izdi*, 2018). Lors de la conclusion d'un contrat électronique, il est nécessaire que le destinataire de l'offre puisse examiner minutieusement les détails de l'ordre ainsi que son prix total. L'idée est de lui permettre de corriger toute éventuelle erreur avant de confirmer l'ordre précité pour manifester son acceptation (Art. 65-5 du DOC).

En principe, la signature d'un acte juridique électronique est essentielle pour identifier son signataire et exprimer son accord avec les obligations découlant de cet acte. Dans la pratique, il est nécessaire de s'assurer que le processus d'identification utilisé est fiable et qu'il établit clairement le lien entre la signature et l'acte auquel elle est associée (Art. 417-2 du DOC).

En droit marocain, l'utilisation de la signature électronique est soumise à certaines conditions. Tout d'abord, la personne qui utilise la signature électronique doit être en mesure de prouver qu'elle est bien l'auteur de la signature électronique. En outre, la signature électronique doit être liée aux données électroniques de manière à permettre la vérification de l'intégrité des données. Pour garantir cette sécurité, il est recommandé d'utiliser des prestataires de services de confiance reconnus par l'État marocain. La cryptographie joue un rôle crucial en la matière dans la mesure où elle fournit un système de codage protégeant les logiciels et les programmes contre les procédés de fraude informatique (*Balga*, 2014). En d'autres termes, elle permet de garantir la sécurité et l'intégrité des données électroniques en utilisant des techniques de chiffrement avancées.

La loi n°53-05 relative à l'échange électronique de données juridiques admet l'existence d'une signature électronique simple et d'une signature électronique sécurisée. La signature électronique simple est la forme de signature électronique la plus courante, elle consiste en la simple inscription du nom de l'auteur de la signature électronique. Il s'agit d'une pratique courante telle que les processus de transmission de documents numériques dans une entreprise. Toutefois, lorsqu'il s'agit de traiter avec les administrations, il est plus fréquent d'utiliser une signature électronique sécurisée (*Kettani*, 2022). Selon l'article 417-3 du Dahir des Obligations et des Contrats : « *Une signature électronique est considérée comme sécurisée lorsqu'elle est créée, l'identité du signataire assurée et l'intégrité de l'acte juridique garantie, conformément à la législation et la réglementation en vigueur en la matière* ». Pour être valable, elle doit respecter certaines conditions à savoir :

- Etre spécifique à l'auteur de la signature ;
- Etre générée par des moyens que le signataire peut garder sous son contrôle exclusif ;
- Garantir un lien avec le document auquel elle est attachée, de sorte que toute modification ultérieure du document puisse être détectée.

Il y a lieu de préciser que le signataire peut être une personne physique agissant soit pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente (Art. 7 de la loi n°53-05). Il met en place un dispositif de création de signature électronique prenant la forme d'un matériel et/ou un logiciel mettant en œuvre les données de création de signature électronique avec l'ensemble des éléments permettant de distinguer le signataire. C'est en ce sens selon l'arrêt de la Cour de Cassation rendu le 29 janvier 2019, l'absence de signature électronique, de cachet et de date rend caduque une convocation de salarié envoyée par courrier électronique[2].

La vérification de la signature électronique se fait *via* des données mentionnées dans le certificat électronique. La certification électronique est le processus qui permet de vérifier l'authenticité de la signature électronique. Elle consiste en la délivrance par un tiers de confiance, appelé "*prestataire de services de certification électronique*", d'un certificat électronique qui atteste de l'identité du signataire, de l'existence de sa clé publique, de la validité de la signature électronique et de la date et heure de la signature.

Le certificat électronique peut être simple tout comme sécurisé (Art 10 de la loi n°53-05). Celui-ci doit être délivré par un prestataire de services de certification électronique agréé par l'Autorité nationale d'agrément et de surveillance de la certification électronique (Art 11 de la loi n°53-05). Ce dernier doit respecter certaines obligations légales en matière de sécurité, de confidentialité et d'intégrité des données. A l'heure actuelle, la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) a agréé Barid eSign comme l'unique prestataire de services de certification électronique au Maroc[3]. La signature électronique émise par Barid @sign est valable exclusivement sur le territoire marocain et ne peut être utilisée pour les contrats internationaux soumis à un tribunal étranger.

Parmi les mentions qui doivent figurer dans le certificat électronique on trouve l'identité du prestataire de services de certification électronique outre la dénomination de l'Etat dans lequel il est établi. Le certificat doit également comporter un code d'identité et une mention précisant sa délivrance à titre de certificat électronique sécurisé. Il doit impliquer en plus signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique mais aussi les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé (Art. 11 de la loi n°53-05). D'autres indications sont également nécessaires telles que l'identification du signataire, la date du début et de la fin de validité du certificat électronique ainsi que les données permettant de vérifier la signature électronique sécurisée.

Par ailleurs, dès que les données nécessaires pour créer une signature électronique sont générées, la responsabilité de garantir la confidentialité et l'intégrité de ces données revient entièrement au titulaire du certificat électronique. Toute utilisation de ces données est considérée comme étant effectuée par le titulaire, à moins qu'il ne puisse prouver le contraire (Art 25 de la loi n°53-05). Le détenteur du certificat électronique est obligé de signaler au prestataire de services de certification toute modification des informations prévues

[2] Arrêt de la Cour de Cassation n°147, dossier n°858/5/1/2018, rendu le 29 janvier 2019

[3] http://www.baridesign.ma/wps/portal/barideSign, consulté le 06/09/2022

dans le certificat, dès que possible (Art. 26 de la loi n°53-05).

2/ La signature électronique en tant que moyen de preuve

La preuve, au sens juridique, est l'établissement de la preuve de l'existence d'un fait juridique devant le pouvoir judiciaire selon les modalités prévues par la loi (*Al-Hasnaoui*, 2015). Les règles de preuve varient en fonction du domaine concerné. En droit civil et commercial, ce sont les parties qui doivent fournir les preuves qu'elles détiennent au juge.

En ce qui est de la signature électronique, il s'agit de démontrer que le signataire est bien celui qu'il prétend être et qu'il a effectivement signé le document en question (Art 417-2 du DOC). Pour se faire, il convient de préciser que l'article 417-du DOC 1 dispose que : « *L'écrit sur support électronique a la même force probante que l'écrit sur support papier* ». Il en résulte que la signature électronique a la même force probante que la signature manuscrite (*Berkchi*, 2021). La loi n°53-05 relative à l'échange électronique de données juridiques exige que la signature électronique soit liée aux données électroniques de manière à permettre la vérification de l'intégrité des données. En outre, la personne qui utilise la signature électronique doit être en mesure de prouver qu'elle est bien l'auteur de la signature électronique. Pour garantir ce point, il convient non seulement d'identifier la personne dont elle émane mais aussi que le document soit conservé dans des conditions offrant sa garantie intégrale. Comme précédemment invoqué, l'utilisation d'un procédé fiable d'identification est fondée sur le système de certification électronique instaurée par la loi marocaine.

En cas de litige, la preuve de la signature électronique peut être apportée par tous moyens, y compris par tout mode de preuve admis par la loi, à condition que l'intégrité et l'authenticité de la signature électronique soient préservées. Lorsqu'il s'agit d'une signature électronique sécurisée, la fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve contraire. C'est en ce sens que l'article 417-3 dispose que : « *Tout acte sur lequel est apposée une signature électronique sécurisée et qui est horodaté a la même force probante que l'acte dont la signature est légalisée et de date certaine* ». Toutefois, bien que l'email et le fax soient des moyens de preuve, ils ne disposent pas de la force probante qu'un document électronique établi avec une signature électronique sécurisée (SE). De plus, il est possible de falsifier le contenu d'un fax sans détection, tant que l'original n'est pas disponible. En fin de compte, la force probante de ces moyens de preuve est à la discrétion du juge, avec des règles spécifiques pour les affaires commerciales, qui sont régies par l'article 334 du code de commerce et où la preuve est libre. En l'occurrence, conformément à l'arrêt n°730 du 27/6/2007 de la Cour de Cassation, l'utilisation du fax est considérée comme une preuve valide pour démontrer que l'autre partie a été informée de l'envoi ou de la réception de la marchandise, à condition que la réception du fax soit établie devant le tribunal. Par ailleurs, la Cour de Cassation a également rappelé dans son arrêt rendu le 25/11/2015 que sur la base de l'article 417-3 du DOC, le document électronique est accepté comme moyen preuve à condition qu'il soit possible d'identifier légalement la personne qui l'a émis, qu'il soit préparé et conservé conformément aux conditions garantissant son intégrité, et qu'il ait respecté les exigences de l'article en question[4].

Les personnes intéressées peuvent utiliser les copies d'un acte juridique sous forme électronique comme moyen de preuve

[4] Arrêt de la Cour de Cassation n° 2015/390 rendu le 25/11/2015

pourvu que l'acte soit conforme aux articles 417-1 et 417-2 du DOC et que le procédé de conservation de l'acte offre la possibilité d'y accéder. Les conventions et faits juridiques dont le but est de créer, de transférer, de modifier ou d'éteindre des obligations ou des droits, et excédant la somme ou la valeur de dix mille dirhams, peuvent être conclus en acte authentique ou sous seing privé, éventuellement établi sous forme électronique ou transmis par voie électronique (Art. 443 du DOC).

II- La signature électronique comme dispositif de sécurité

La nouvelle loi n°43-20 relative aux services de confiance pour les transactions électroniques promulguée par le Dahir n° 1-20-100 a été publiée au Bulletin officiel du 11 janvier 2020 afin de promouvoir l'utilisation de la signature électronique dans les transactions électroniques et de renforcer la sécurité juridique de ces transactions. Le décret d'application de la loi n°43-20 a été rendu public dans l'édition générale du "Bulletin officiel" n°7160 en date du 12 janvier 2023, et dans sa version officielle en français dans le "Bulletin officiel" n°7162 daté du 19 janvier 2023. Il prendra effet 6 mois après la date de sa publication et abroge le décret n° 2-08-518 du 25 Joumada I 1430 (21 mai 2009) pris pour l'application des articles 13, 14, 15, 21 et 23 de la loi n° 53-05 relative à l'échange électronique des données juridiques.

1/ Une protection renforcée des données numériques

La loi n°43-20 relative aux services de confiance pour les transactions électroniques vise « *fixer le régime applicable aux services de confiance pour les transactions électroniques, aux moyens et prestations de cryptologie ainsi qu'aux opérations effectuées par les prestataires de services de confiance et les règles à respecter par ces derniers et les titulaires des certificats électroniques. Elle fixe également les prérogatives de l'Autorité nationale des services de confiance pour les transactions électroniques, désignée par voie réglementaire et appelée dans la présente loi par Autorité nationale* » (Art. 1 de la loi n°43-20). L'objectif est de garantir les différentes données à caractère personnel en les traitant de manière légale, loyale et transparente, et en protégeant les droits des personnes physiques dont les données sont traitées.

La nouvelle loi établit le régime applicable aux services de confiance pour les transactions électroniques et aux moyens et prestations de cryptologie.

Elle précise également un certain nombre de principes clés pour le traitement des données à caractère personnel, tels que le consentement de la personne concernée, la finalité légitime du traitement, la minimisation des données collectées et la sécurité des données. Les données à caractère personnel se réfèrent à toute information se rapportant à une personne physique identifiée ou identifiable, telle que son nom, son adresse, son numéro de téléphone, son adresse électronique, son adresse IP ou sa localisation géographique.

Elle précise également les droits des personnes concernées dont notamment le droit d'accéder à leurs données, le droit de rectification, le droit à l'effacement et le droit à la portabilité des données (Art 31 de la loi n° 43-20).

Par ailleurs, cette réglementation impose des obligations spécifiques aux prestataires de services de confiance, tels que l'obligation d'employer du personnel, l'obligation d'utiliser des systèmes, matériels et logiciels fiables et assurer leur sécurité technique et la fiabilité des processus pris en charge. Elle s'applique à tous les traitements de données à caractère personnel effectués au Maroc, qu'ils soient réalisés par des entités publiques ou

privées. Elle vise également les traitements effectués par des entités situées hors du Maroc, à condition qu'ils concernent des personnes physiques situées sur le territoire marocain.

La nouvelle loi définit plusieurs types de signatures électroniques reconnues juridiquement au Maroc. Voici un aperçu de ces différents types :

1. **La signature électronique simple** se rapproche de celle instaurée par la loi n° 53-05. Selon les dispositions de l'article 2 de la loi n°43-20, elle porte sur « *l'usage d'un procédé fiable d'identification électronique garantissant le lien avec l'acte auquel la signature s'attache et qui exprime le consentement du signataire* ». Cette forme de signature électronique consiste en l'utilisation d'un code confidentiel ou d'un mot de passe pour authentifier un document électronique. Elle est souvent utilisée pour des transactions à faible risque, telles que la confirmation d'un abonnement en ligne ou la validation d'un formulaire.
2. **La signature électronique avancée** : Cette forme de signature électronique est plus sécurisée que la signature électronique simple, car elle utilise des éléments supplémentaires pour garantir l'authenticité du document électronique. Elle peut inclure l'utilisation d'un certificat électronique, d'un dispositif de sécurité spécifique ou d'une signature biométrique pour authentifier la signature. En plus d'être propre au signataire, elle doit permettre d'identifier le signataire et être créée *via* des données que seul le signataire peut utiliser sous son contrôle exclusif. En outre, elle doit garantir l'intégrité du document électronique, c'est-à-dire que toute modification apportée au document doit être détectable.
3. **La signature électronique qualifiée** repose sur les transactions rares et complexes. Celle-ci est la forme de signature électronique la plus sécurisée, car elle est liée à un certificat électronique qualifié délivré par un prestataire de services de confiance. D'une part, elle doit être produite par un dispositif qualifié de création de signature électronique et de l'autre elle doit reposer sur un certificat qualifié de signature électronique (Art. 6 de la loi 43-20). Elle est considérée comme juridiquement équivalente à une signature manuscrite et offre le plus haut niveau de sécurité. Elle garantit non seulement l'authenticité et l'intégrité du document électronique, mais aussi l'identification de la personne qui a apposé sa signature. En ce sens, Le prestataire de services de confiance qui souhaite émettre des certificats électroniques qualifiés doit s'engager à vérifier l'identité et toutes les informations pertinentes relatives à la personne physique ou morale à qui il délivre le certificat. Cette vérification peut être effectuée de plusieurs façons soit par la présence en personne de la personne physique ou du représentant autorisé par la personne morale soit par des moyens d'identifications électroniques fixés par voie réglementation. Parmi d'autres moyens de vérification figure l'utilisation d'un certificat électronique ou de cachet électronique qui a été préalablement délivré à une personne dont l'identité a été vérifiée voire l'utilisation d'autres méthodes d'identification qui

offrent une garantie jugée équivalente en termes de fiabilité quant à la présence physique, et qui sont considérées comme telles par l'autorité nationale compétente.

De ce qui précède, il convient de préciser que la loi n°43-20 prévoit que toute signature électronique doit être liée de manière univoque à la personne qui l'a apposée et doit être sous le contrôle exclusif de cette personne. La loi précise également que la forme de signature électronique utilisée doit être proportionnelle aux risques associés à la transaction électronique. Ainsi, il est recommandé d'utiliser une signature électronique qualifiée pour les transactions les plus importantes et les plus risquées, tandis qu'une signature électronique simple peut être suffisante pour les transactions de faible valeur ou à faible risque. En ce sens, il convient de noter que le fait d'utiliser la signature électronique comme moyen de preuve devant la justice ne peut être refusée pour la simple raison qu'elle soit électronique ou qu'elle ne réponde pas aux exigences d'une signature électronique qualifiée (Art. 7 de la loi n°43-20).

2/ De l'autorité nationale des services de confiance pour les transactions électroniques

Face à l'utilisation croissante des technologies numériques, la loi 43-20 a été l'occasion de renforcer les attributions et missions de l'autorité nationale des services de confiance pour les transactions électroniques. Celle-ci a pour objectif de superviser les prestataires de services de confiance électroniques. Ces derniers sont des services qui permettent d'identifier de manière sûre et fiable les parties impliquées dans une transaction électronique, d'assurer l'intégrité et la confidentialité des données échangées et de garantir la non-répudiation des transactions. Ces services comprennent notamment les signatures électroniques, les sceaux électroniques, les autorités de certification, les prestataires d'horodatage électronique et bien d'autres.

L'Autorité nationale des services de confiance pour les transactions électroniques encourage la confiance dans l'environnement numérique et favorise la création d'un marché des services de confiance électroniques compétitif et innovant. Elle travaille en étroite collaboration avec les acteurs du marché des services de confiance électroniques pour améliorer la qualité des services proposés et réduire les coûts pour les utilisateurs.

L'Autorité nationale a pour mission de superviser ces prestataires de services de certification électronique et de s'assurer qu'ils respectent les exigences légales en matière de sécurité et de fiabilité des services de confiance électroniques (Art.52 et 54 de la loi 43-20). Elle est également chargée de délivrer les certificats de conformité aux prestataires de services de confiance qui répondent aux normes de sécurité et de fiabilité. Elle propose également les projets de textes législatifs et réglementaires relatifs aux services de confiance pour les transactions électroniques.

Enfin, l'Autorité nationale est habilitée à vérifier la conformité des activités d'un prestataire de services de confiance électroniques avec les lois et règlements applicables. Cette vérification peut être effectuée sur demande ou à l'initiative de l'autorité elle-même. Des experts peuvent être sollicités pour aider l'autorité dans sa mission de contrôle. Les coûts liés à ces opérations sont à la charge du prestataire de services de confiance (Art. 55 de la loi 43-20).

CONCLUSION

En conclusion, le droit marocain reconnaît la validité de la signature électronique et

des contrats électroniques. Cependant, l'utilisation de la signature électronique est soumise à certaines conditions et les parties doivent s'assurer que les conditions de formation du contrat sont respectées.

La preuve de la signature électronique telle que prévue par la loi n°53-05 relative à l'échange électronique de données juridiques repose sur l'utilisation d'un certificat électronique délivré par un prestataire de services de certification électronique, qui permet d'attester de l'identité du signataire, de la validité de la signature électronique et de la date et heure de la signature. En cas de litige, la preuve de la signature électronique peut être apportée par tous moyens, à condition que l'intégrité et l'authenticité de la signature électronique soient préservées.

Par ailleurs, la nouvelle loi n°43-20 relative aux services de confiance pour les transactions électroniques établit un cadre juridique solide pour la protection des données à caractère personnel au Maroc. Elle renforce les droits des personnes concernées et établit des obligations spécifiques pour les prestataires de services de confiance.

L'Autorité nationale des services de confiance pour les transactions électroniques, de son côté, est une institution clé dans le développement d'un environnement numérique sûr et fiable au Maroc. Elle joue un rôle important dans la promotion de la confiance dans l'économie numérique et la protection des droits des consommateurs et des utilisateurs de services électroniques.

Pour conclure, il convient de préciser que la sécurité numérique est un enjeu crucial de notre époque. L'État peut garantir la sécurité numérique en adoptant une approche multi-facettes qui comprend la réglementation, la sensibilisation, la collaboration, la formation et la surveillance. La mise en place des différentes réglementations a pour objectif d'obliger les entreprises et les organisations à prendre des mesures de sécurité numérique appropriées pour protéger les données des utilisateurs. Recourir à des campagnes de sensibilisation pourra également informer les citoyens et les entreprises sur les menaces et les risques de sécurité numérique. Ces campagnes de sensibilisation pourront inclure des conseils pratiques pour protéger les données, des avertissements sur les escroqueries et les phishing, voire des informations sur les dernières tendances en matière de sécurité numérique. En parallèle, l'Etat pourra collaborer avec différentes structures pour identifier les menaces et les vulnérabilités et mettre en place des mesures de sécurité appropriées. Il pourra investir en outre dans la formation de professionnels de la sécurité numérique pour s'assurer que les entreprises et les organisations ont accès aux compétences nécessaires en la matière. Enfin, la surveillance des réseaux et des divers systèmes sert à détecter les menaces, les attaques de sécurité numérique et la collecte de données sur les incidents pour mieux comprendre les tendances et les risques de sécurité numérique.

BIBLIOGRAPHIE

Al-Hasnaoui M 2015, « Al-Ithbât fî Al-Aqd Al-iliktrônî », manchourât Majallat Al-Oloum Al-Qanouniya.

Alassaire S 2015, « Contrat et signature électroniques : Portée du cadre juridique », Alassaire Juriconseil

Al-Rachadî H 2022, « Attahawol Arraqmî limarfaq Al-Adpala bi Al-Maghreb », Majallat Al-Bâhitch li Dirassât wa Al-Abhâth Al-Qanouniya wa Al-Qadaeia, Manchourât Mawqi' Al-Bahith, Raqm 45

Balga H 2014, « La sécurité juridique dans le commerce électronique au Maroc », Revista de estudio Fronterizos Del Estrecho De Gibraltar

Berkchi S 2021, « L'acte électronique au Maroc : Etude de Cas de l'acte notarié électronique », *Revue Internationale du Chercheur, vol.* 2, n°3

De Lamberterie I 2006, « La valeur juridique de la signature, perspective de longue durée », Hypothèses

Huet J 2021, « Contrat électronique », Fascicule 2418, JurisClasseur Contrats-Distribution

Izdi S 2018, « La preuve du contrat électronique en droit marocain », Revue marocaine du droit commercial et des affaires, numéro double 4-5

Kettani M 2022, « le cadre juridique et les applications pratiques de la signature électronique au Maroc », intervention faite lors de la 4ème édition du Casablanca Business Law Forum, organisé 13 décembre 2022

Ngombé Y 2022, « Les contrats électroniques », Fiches de Droit du numérique, Ellipses

Rahajaritsimba FM 2022, « L'authenticité et l'intégrité de la signature électronique » Journal of Integrated Studies In Economics, Law, Technical Sciences & Communication Vol. l, N°1, 2022

Recueils juridiques

Arrêt de la Cour de Cassation n°147, dossier n°858/5/1/2018, rendu le 29/01/2019

Arrêt de la Cour de Cassation n° 2015/390 rendu le 25/11/2015

Arrêt de la Cour de Cassation n°730 du 27/6/2007

Dahir formant code des obligations et des contrats.

Dahir n°1-07-129 kaada 1428 (30 novembre 2007) portant promulgation de la loi n°53-05 relative à l'échange électronique de données juridiques.

Dahir n°1-20-100 du 16 joumada I 1442 (31 décembre 2020) portant promulgation de la loi n°43-20 relative aux services de confiance pour les transactions électroniques.

Décret d'application de la loi n°43-20 relative aux services de confiance pour les transactions électroniques.

Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation, 2001.