L'AUTHENTICITÉ ET L'INTÉGRITÉ DE LA SIGNATURE ÉLECTRONIQUE

RAHAJARITSIMBA Franckie Mahery
Doctorante en Droit privé
Faculté des Sciences Juridiques, Economiques et Sociales de Fès
Laboratoire ESSOR, Droit, philosophie et Société
Encadrée par le
Professeur MARGHICH Abdellah
Courriel:franckie.rahajaritsimba@gmail.com

Résumé :

Cet article analyse l'authenticité et l'intégrité de la signature électronique au Maroc en mettant un accent sur la reconnaissance d'un écrit électronique au temps de la loi n°53-05 relative à l'échange électronique de données juridiques et les apports de la loi n°43-20 relative aux services de confiance pour les transactions électroniques. Il démontre un aperçu de la cryptographie pour permettre de comprendre le processus de création et d'utilisation de la signature électronique. L'analyse met en évidence la différence et le rôle du certificat de conformité, du certificat électronique, de l'autorité nationale d'agrément et de surveillance de la certification électronique et des prestataires de service de certification électronique.

Abstract :

This article analyses the authenticity and integrity of the electronic signature in Morocco, focusing on the recognition of an electronic document at the time of Law No. 53-05 on the electronic exchange of legal data and the contributions of Law No. 43-20 on trust services for electronic transactions. It provides an overview of cryptography to help understand the process of creating and using electronic signatures. The analysis highlights the difference and the role of the certificate of conformity, the electronic certificate, the national authority for the approval and supervision of electronic certification and the electronic certification service providers.

Mots-clés :

Signature électronique, cryptographie, certificat de conformité, certificat électronique.

Introduction

La conclusion de contrat est un acte que nous effectuons tous au quotidien. Bien que la loi n'exige de formalisme que pour la conclusion de certains contrats spécifiques, les parties préfèrent de plus en plus établir un écrit. Il offre une sécurité juridique aux parties et sert de repère en cas de survenance d'un événement. Le contrat étant un accord de volonté qui tend à produire des effets juridiques entre les parties, il est conditionné par leur capacité, leur consentement, un objet et une contrepartie[1]. Lorsque les parties ne parviennent pas à régler leur différend de manière amiable, celui-ci est porté devant la juridiction compétente. Pour le juge, le contrat est une preuve tandis que pour les parties, il permet d'appuyer leurs allégations. Pour que la preuve soit recevable et persuasive, elle doit être établie sur un support fiable et indélébile[2]. Le consentement est un point essentiel qui est vérifié par le juge car elle détermine si le contrat est valide. Selon l'article 417-2 du dahir formant code des obligations et des contrats, « la signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose et exprime son consentement aux obligations qui découlent de cet acte ». La signature permet de vérifier donc l'identité et le consentement de la personne.

La signature manuscrite est celle que nous connaissons tous et qui est la plus utilisée actuellement au Maroc. Lorsqu'elle est apposée sur un contrat, le juge doit avoir la garantie sur l'identité de la personne qui l'a apposé, c'est ce qu'on appelle l' « authenticité ». Normalement, une signature ne doit pas pouvoir être reproduite que par son titulaire et toute personne doit être en mesure de vérifier que telle signature appartient bien à telle personne. Concernant le premier point, il n'y a aucune garantie car une autre personne peut très bien reproduire une signature qui ne lui appartient pas. Quant au second point, la vérification se fait souvent à l'aide d'une carte d'identité ou un passeport qui contient la signature de l'individu. Selon la jurisprudence marocaine, un acte sous seing privé est un moyen de preuve tant que la signature n'a pas été désavouée[3]. Si ce cas de figure se produit, le juge peut faire appel à un expert pour examiner la signature manuscrite. Cependant, l'authenticité de la signature manuscrite reste discutable, de plus, une personne ne peut pas apposer exactement la même signature partout. C'est pour ces raisons que la loi marocaine exige que la signature manuscrite soit apposée devant un officier public habilité à certifier pour conférer l'authenticité à cette dernière[4]. Pour certains actes, la légalisation de la signature est obligatoire au Maroc[5].

---

[1] Article 2 et suivants du Dahir des Obligations et des Contrats déterminant les éléments nécessaires à la validité des obligations.

[2] IZDI (Sana), La preuve du contrat électronique en droit marocain, Revue marocaine du droit commercial et des affaires, numéro double 4-5, 2018, p. 98 – 104.

[3] Arrêt de la Cour de cassation de Rabat n°9,dossier n°100/2/1/2005, en date du 04/01/2006.

[4] Article 417-2 dahir formant code des obligations et des contrats.

[5] Au Maroc, un contrat de travail qui n'a pas été établi en deux exemplaires et ne comportant pas les signatures légalisées du salarié et de l'employeur doit être écarté. Arrêt de la Cour de cassation de Rabat n° 737/5/1/2007 en date du 21/05/2018.
Au Maroc, la démission doit comporter une signature légalisée. Arrêt de la Cour de cassation de Rabat, chambre sociale,dossier n°1442/5/1/2017, n°244 en date du 28/03/2018.

En plus de la signature manuscrite, nous pouvons également utiliser la signature électronique. En effet, grâce à l'évolution technologique, nous pouvons désormais signer des documents par voie électronique ce qui nous permet de conclure des contrats rapidement et à distance. Nous pouvons constater par exemple que les banques font de plus en plus recours à l'utilisation de ce type de signature pour les opérations à faible valeur ajoutée car elle est moins onéreuse, plus fiable et fait gagner du temps[6]. Les banques ont même étendu son utilisation à la gestion des ressources humaines. Dans une telle situation, une convocation du salarié à travers un courrier électronique est nulle si elle ne contient pas une signature électronique, un cachet et une date[7]. Ceci-dit, le formalisme électronique peut être écarté dans les contrats conclus exclusivement par échanges de courriers électroniques et dans les contrats liant des professionnels[8] par exemple. Comme la signature manuscrite, nous nous posons la question de l'authenticité de la signature électronique. Pour qu'un acte contenant une signature électronique soit authentique, la législation marocaine précise qu'il convient d'utiliser un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache[9]. L'authenticité est importante car elle octroie la force probante, c'est à dire, la capacité à servir de moyen de preuve[10]. En outre, la signature électronique est le seul type de signature qui offre une garantie sur l'intégrité. Dans le cadre de cette étude, nous allons donc nous pencher sur l'authenticité et l'intégrité de la signature électronique.

Avant d'aller plus loin, il est à noter que l'authenticité est la certitude du destinataire sur l'identité de l'expéditeur et l'intégrité la certitude du destinataire que le message n'a pas été modifié en cours de route[11]. Quant à la signature électronique, elle peut être définie comme une « signature qui consiste en 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 »[12]. Elle est aussi définie par la loi type de la Commission des Nations Unies pour le Droit Commercial International (CNUDCI) comme « des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue. »[13] L'authenticité et l'intégrité de la signature électronique peuvent donc être définies comme les éléments nécessaires pour qu'un document comportant une signature électronique puisse servir de preuve valable devant la juridiction compétente.

---

[6] Pascal Colin, « Les gains de productivité avec la signature électronique sont impressionnants », Docusign, Briefing technologies bancaires, avril 2016, p.12-13.

[7] Arrêt de la Cour de Cassation n°147, dossier n°858/5/1/2018, en date du 29/01/2019.

[8] ERAL-SCHUHL (Christiane), Cyberdroit - Le droit à l'épreuve de l'internet, collection Praxis Dalloz, 8ème édition Dalloz, 2020, 1888 p.

[9] Article 417-2 dahir formant code des obligations et des contrats.

[10] https://www.droit.fr/definition/2081-force-probante/ , consulté le 22 juillet à 20h06.

[11] L'informateur, Sécurité 6 : Protocoles Cryptographiques, https://www.youtube.com/watch?v=25HbXbccPUY&t=319s

[12] Article 2 du 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.

[13] Article 2 de la loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation, 2001.

Historiquement, internet est devenu accessible au grand public dans les années 90, les messageries électroniques sont apparues mais la jurisprudence excluait toute preuve électronique à cette époque, contrairement à nos jours où les moyens électroniques sont considérés comme moyens de preuve devant les juridictions[14]. La promulgation de la directive européenne 1999/93/CE sur la signature électronique du 13 décembre 1999 officialise la reconnaissance de la signature électronique en Europe et lui attribue la même valeur que la signature manuscrite. Au Maroc, c'est en 2007 que la loi n°53-05 relative à l'échange électronique de données juridiques est apparue pour réglementer le cadre légal de la signature électronique et pour lui attribuer la force probante sous certaines conditions. En décembre 2020, la loi n°43-20 relative aux services de confiance pour les transactions électroniques est venue apporter des compléments aux dispositions légales existantes.

Notre sujet a un intérêt théorique car le fait d'apporter des clarifications et précisions sur l'authenticité et l'intégrité de la signature électronique permettra aux utilisateurs de connaître et faire prévaloir leurs droits ; il permettra également aux utilisateurs de mieux choisir le type de signature électronique à utiliser dès le départ.

Notre sujet a également un intérêt pratique car la signature électronique est devenue incontournable de nos jours. Si auparavant il était intéressant de l'avoir pour signer un contrat à distance et ainsi gagner en temps ; actuellement, il est presque indispensable de l'avoir en raison de la vulgarisation du commerce électronique et de la proposition de prestation de services en ligne ainsi que de la pandémie du covid19 qui a multiplié et accéléré la dématérialisation de plusieurs procédés.

La question qui se pose est la suivante : quelle est la valeur juridique de la signature électronique ?

Afin de répondre à cette question, il serait convenable d'aborder tout d'abord les aspects techniques de la signature électronique (1) avant d'étudier ses aspects juridiques (2).

1. Les aspects techniques de la signature électronique

La signature électronique n'est pas une nouveauté en tant que telle mais son utilisation reste encore occasionnelle. De ce fait, elle prête souvent à confusion. C'est pour cette raison qu'il est important de signaler dès le départ qu'une signature manuscrite numérisée, une signature manuscrite apposée sur un support électronique comme une tablette ou les noms saisis au clavier sont des signatures numériques existantes[15] mais ne sont réglementées par aucun texte de loi, nous ne les considérerons donc pas comme une signature électronique. Mais qu'est-ce qu'une signature électronique alors ? Pour comprendre sa nature, il convient d'étudier la manière dont elle est conçue et de connaître le dispositif de création utilisé (1.1) ; il serait également convenable d'étudier le cadre juridique qui réglemente ce dispositif de création (1.2).

[14] Arrêt de la Cour de cassation n°521, dossier n°2390/5/1/2016, en date du 05/05/201.

[15] COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL (CNUDCI), Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques, Publicaiton des Nations Unies, Vienne, 2009

1.1. Le dispositif de création de la signature électronique

Selon l'article 8 de la loi n°53-05 relative à l'échange électronique des données juridiques, une clé cryptographique privée peut être utilisée pour créer une signature électronique, il s'agit donc du dispositif de création de la signature électronique. Etymologiquement, « cryptographie » signifie « écrire de manière cachée ». En effet, elle consiste à chiffrer un message dans le but d'atteindre une sécurité informatique élevée.

La signature électronique peut être conçue à partir d'un système de cryptographie asymétrique. Ce système fonctionne de la manière suivante : il faut deux clés : la première clé est une clé publique pour chiffrer, elle peut être connue par tout le monde ; la seconde clé est une clé privée pour déchiffrer, elle peut être connue uniquement de celui qui la possède. Quand une personne chiffre un message avec sa clé publique, on ne peut déchiffrer ce message qu'avec sa clé privée ; notons aussi qu'il n'est pas possible de trouver la clé privée à partir de la clé publique.

Deux systèmes de cryptographie asymétrique peuvent être utilisés pour concevoir une signature électronique : le système RSA et le système El-Gamal[16]. Le système RSA a été inventé en 1978 par Rivest, Shamir et Adleman. « Il utilise une fonction à sens unique avec clés privées – secrètes – permettant l'inversion de la fonction par celui connaissant ces clés privées. Il est basé sur la difficulté de factoriser un nombre qui est le produit de deux grands nombres premiers »[17]. Le système RSA est basé sur la factorisation, quant au système El-Gamal, il est basé sur le logarithme discret. Le chiffrement d'El-Gamal a été inventé en 1982 par Taher ElGamal. C'est une méthode de cryptographie à clé publique dont la sécurité repose sur la difficulté de calculer le logarithme discret[18].

Afin de mieux comprendre le fonctionnement de la cryptographie asymétrique, voici un exemple[19] :

- A veut envoyer un message à B et lui demande sa clé publique.
- B répond et demande la clé publique de A également.
- A envoie sa clé publique à B.
- A chiffre le message et la signature avec la clé publique de B pour obtenir le texte.
- B reçoit le texte et déchiffre le message et la signature de A grâce à sa clé privée.
- B utilise la clé publique de A pour vérifier la signature de A.
- Si la signature est correcte, B sait que le message a bien été écrit par A et qu'il n'a pas été modifié en chemin.

[16] L'informateur, Sécurité 5 : Signatures Digitales, https://www.youtube.com/watch?v=t3pzkDRgQW8&t=30s

[17] M. Bigarré, D. Leroy, L. Valat, Cryptographie : système RSA.

[18] https://elearning-facsci.univannaba.dz/pluginfile.php/13922/mod_resource/content/0/CHAP2.3_%20El%20Gamal.pdf , consulté le 26/07/2021 à 13h24.

[19] L'informateur, Sécurité 6 : Protocoles Cryptographiques, https://www.youtube.com/watch?v=25HbXbccPUY&t=319s

A ce stade, la signature électronique a deux propriétés : l'authenticité qui garantit l'identité de l'expéditeur et l'intégrité qui garantit le contenu du message. Si le message a été modifié, il ne sera pas reconnu comme correcte pendant la vérification avec la clé publique.

Pour atteindre un niveau de sécurité informatique encore un peu plus élevé, nous pouvons faire en sorte que la signature électronique ait également comme propriété la confidentialité. Elle garantit qu'aucun attaquant ne puisse voir le message entre l'expéditeur et le destinataire. Afin de réponde à l'authenticité, l'intégrité et la confidentialité, il faut un cryptosystème qui consiste à combiner la cryptographie asymétrique et symétrique[20]. Il est possible d'utiliser des protocoles comme l' « authenticated key exchange (AKE) »[21] ou encore le « Hash-based Message Authentification Code »[22].

En un mot, la signature électronique utilise la cryptographie pour créer deux clés différentes mais mathématiquement liées entre elles. Une clé est utilisée pour créer une signature électronique et transformer des données en forme inintelligible et l'autre pour vérifier la signature électronique et pour restituer le message dans sa forme initiale. En plus des deux clés susmentionnées, il y a aussi la fonction de hachage qui est utilisée pour créer et vérifier la signature électronique. Elle permet d'assurer qu'aucune modification n'a été apportée au message depuis que ce dernier a été signé sous forme numérique[23].

Sans trop rentrer dans les détails techniques, retenons que la cryptographie permet la conception de la signature électronique et lui attribue l'authenticité, l'intégrité et la confidentialité. Nous nous demandons alors quel cadre juridique réglemente la cryptographie.

1.2. Le cadre juridique de la cryptographie

L'utilisation des moyens de cryptographie et l'offre de prestation de cryptographie sont règlementées par les articles 12 à 14 de la loi n°53-05 relative à l'échange électronique de données juridiques. Selon cette loi, les moyens de cryptographie[24] sont le logiciel qui est conçu ou modifié pour transformer des données pour réaliser l'opération inverse. Il a pour rôle de garantir la sécurité de l'échange et du stockage des données juridiques par voie électronique. Quant à la prestation de cryptographie[25], c'est l'opération qui vise l'utilisation des moyens de cryptographie pour le compte d'autrui.

---

[20] L'informateur, Sécurité 6 : Protocoles Cryptographiques, https://www.youtube.com/watch?v=25HbXbccPUY&t=319s

[21] W. Diffie, P. Van Oorschot, M. Wiener, Authentication and authenticated key exchanges. Designs, Codes and Cryptography, juin 1992

[22] Mihir Bellare, Ran Canetti et Hugo Krawczyk, Keying, Hash Functions for Message Authentication, CRYPTO 1996, p. 1–15.

[23] COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL (CNUDCI), Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques, Publicaiton des Nations Unies, Vienne, 2009

[24] Article 12 paragraphe 1 du 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.

[25] Article 12 paragraphe 3 du 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.

Etant donné qu'il s'agit d'une manipulation technique et qu'il faut rester vigilant concernant les éventuels piratages de toute sorte, le Maroc a soumis l'importation, l'exportation, la fourniture, l'exploitation et l'utilisation de moyens de cryptographie et prestations de cryptographie à une déclaration ou autorisation préalable.

Ainsi, pour préserver la sécurité nationale, seuls les prestataires de services de certification électronique peuvent fournir de moyens ou prestations de cryptographie, à défaut, il faut demander un agrément. Sur la plan international, la CNUDCI ne fait référence à aucun tiers de confiance mais se limite à énumérer les règles de conduite que ce dernier doit adopter[26], ce qui est évident car instaurer un tiers de confiance commun à tous les Etats membres serait matériellement très difficile à faire.

Au Maroc, les prestataires de service de certification électronique sont des sociétés ayant leurs sièges au Maroc. Ils sont agréés par l'autorité nationale d'agrément et de surveillance de la certification électronique et leurs activités sont également contrôlées par cette dernière.

Les prestataires de services de certification électronique doivent satisfaire à certaines conditions pour pouvoir être agréés par l'autorité nationale d'agrément et de surveillance de la certification électronique[27]. Ces conditions permettent par la même occasion de connaître le cadre juridique du dispositif de création de la signature électronique. En effet, les prestataires de service de certification électronique[28] doivent :

- Garantir la sécurité technique et cryptographique des fonctions qu'assurent les systèmes et les moyens cryptographiques qu'ils proposent ;
- Garantir la confidentialité des données de création de signature électronique ;
- Mettre à disposition du personnel qualifié pour fournir des services de certification électronique ;
- Offrir la possibilité de révoquer un certificat électronique délivré ;
- Avoir un système de sécurité propre qui sert à prévenir la falsification des certificats électroniques et à s'assurer que les données de création de la signature électronique correspondent aux données de sa vérification ;
- Avoir un système de conservation électronique de toutes les informations relatives au certificat électronique qui peuvent servir de preuve devant la justice. Ce système de conservation doit garantir que l'introduction ou modification des données soient réservées aux personnes autorisées, que l'accès à un certificat électronique par une personne extérieure ne peut avoir lieu qu'avec le consentement de son titulaire et que toute modification qui peuvent compromettre la sécurité du système puisse être détectée ;
- S'engager à vérifier l'identité de la personne à laquelle le certificat électronique sera délivré, l'informer sur l'utilisation dudit certificat, les modalités de contestation et de

[26] E. CAPRIOLI, Droit international de l'économie numérique, Les problèmes liés à l'internationalisation de l'économie numérique, éd. LexisNexix, 2007, p. 87- 90.

[27] Article 21 du 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.

[28] Article 20 et suivants du 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.

règlement des litiges ; et l'expiration de son certificat au moins soixante jours à l'avance ;

- Souscrire une assurance pour les éventuelles fautes professionnelles ;
- Révoquer le certificat électronique quand celui-ci a été délivré sur la base de fausses informations ou lorsque les informations contenues dans le certificat ne sont plus conformes à la réalité.

Nous pouvons constater que la loi a fixé des conditions techniques et juridiques qui garantissent la sécurité du dispositif de création de signature électronique, de l'utilisation de la signature électronique et de la conservation des données qui y sont afférentes. Parmi ces conditions, nous pouvons constater également que le prestataire de service de certification électronique doit fournir un certificat électronique. Mais de quoi s'agit-il et quel est son rôle ? Afin de répondre à cette question, nous allons passer à présent à l'analyse des aspects juridiques de la signature électronique.

2. Les aspects juridiques de la signature électronique

L'importance de la signature électronique réside dans sa capacité à rendre valable un écrit électronique pour qu'il puisse servir de preuve. S'il est désormais reconnu qu'un écrit électronique a la même force probante qu'un écrit sur papier[29], il reste à savoir si cet écrit est authentique ou non. Un acte authentique est un acte dont la signature a été apposée devant un officier public habilité à certifier quand le support est physique, quand le support est électronique, c'est un acte dont la signature électronique est sécurisée ou qualifiée. Nous allons donc étudier les conditions requises pour qu'une signature électronique puisse être reconnue comme sécurisée ou qualifié mais nous allons aussi nous intéresser à son effet juridique quand ce n'est pas le cas.

2.1. La signature électronique qualifiée

La loi n°53-05 relative à l'échange électronique des données juridiques mentionne uniquement la signature électronique sécurisée et précise les exigences y afférentes. La signature électronique sécurisée doit être propre au signataire, être créée par des moyens que le signataire peut garder sous son contrôle exclusif, garantir un lien avec l'acte auquel elle s'attache pour que toute modification ultérieure soit détectable, être produite par un dispositif

[29] Article 417-1 du dahir formant code des obligations et des contrats.
Cet article respecte le principe de la neutralité technique ou le principe d'égalité de traitement des techniques de signature prévu à l'article 3 de la loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation, 2001. Selon ce principe, à partir du moment où une méthode de création de signature électronique satisfait aux exigences de fiabilité de la loi applicable, la signature doit alors recevoir le même traitement qu'une signature manuscrite.

de création de signature électronique attesté par un certificat de conformité ; et être accompagnée d'un certificat électronique[30].

Le certificat de conformité est délivré par l'autorité nationale d'agrément et de surveillance de la certification électronique. Il garantit que les données de création de signature électronique ne puissent être établies plus d'une fois et que leur confidentialité est assurée, qu'elles ne puissent être trouvées par déduction et que la signature électronique soit protégée de toute falsification et utilisation tierce[31].

Quant au certificat électronique, il est délivré par le prestataire de services de certification électronique comme mentionné plus haut. Il atteste le lien entre les données de vérification de signature électronique et le signataire[32].

En 2020, la loi n°43-20 relative aux services de confiance pour les transactions électroniques mentionne plusieurs types de signature électronique dont la signature électronique qualifiée. C'est une signature électronique qui doit être produite par un dispositif qualifié de création de signature électronique et qui repose sur un certificat qualifié de signature électronique délivré par le prestataire de services[33].

Nous pouvons constater que la signature électronique sécurisée est l'équivalent de la signature électronique qualifiée mais la nouvelle loi a tout simplement modifié sa dénomination. Elle a comme condition particulière de devoir être accompagnée par le certificat de conformité et le certificat électronique.

Dans la pratique au Maroc, pour avoir une signature électronique sécurisée, il convient de se rapprocher de Barid eSign. Ce dernier remet un dispositif certifié sous forme d'une clé cryptographique qui contient un logiciel permettant l'émission d'un certificat électronique sécurisée et la réalisation de signatures électroniques sécurisées[34].

Barid e-Sign est la première plateforme de production de certificats électroniques[35] au Maroc et est la seule pour le moment. Pour se voir délivrer un dispositif de création de signature électronique par cette plateforme, il faut être présent physiquement au Maroc pour le récupérer en personne. Cette démarche pose une limite pour un marocain qui est à l'étranger et qui veut signer un contrat dont un éventuel litige sera jugé au Maroc. Il est à noter que seuls les dispositifs de création de signature électronique délivrés par Barid eSign permettent l'émission de signatures électroniques dont la force probante est reconnue au Maroc. Ainsi, l'usage de cette signature sera écarté pour la conclusion des contrats internationaux conclus avec des

[30] Article 6 du 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.

[31] Article 9 du 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.

[32] Article 10 du 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.

[33] Article 6 du 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.

[34] Clifford Chance, « Utilisation de la signature électronique au Maroc », mai 2020

[35] Site officiel Programme e-gouvernement Royaume du Maroc : http://www.egov.ma/fr/certification-%C3%A9lectronique , consulté le 10/08/2021 à 21h01.

parties étrangères n'ayant pas de représentant au Maroc[36]. Toutefois, si la partie étrangère dispose d'un certificat délivré à l'étranger par un prestataire de services à l'étranger qui émane d'un pays avec qui le Maroc a signé un accord multilatéral ou bilatéral de reconnaissance réciproque, le certificat en question aura la même valeur juridique qu'un certificat délivré par un prestataire de certification électronique établi au Maroc[37]. La force probante d'une signature issue d'un tel certificat sera donc reconnue au Maroc. C'est le principe de non-discrimmination prévue à l'article 12 de la loi type de la CNUDCI[38]. Ce principe prévoit la reconnaissance des signatures et certificats électroniques étrangers. Selon ce principe, le lieu d'origine ne peut être un facteur déterminant pour apprécier la valeur juridique d'une signature ou d'un certificat. Si ces derniers présentent un niveau de fiabilité substantiellement équivalent sur la base des normes internationales reconnues, ils peuvent être reconnus à l'étranger. Il est à noter qu'actuellement, l'équivalence des signatures électroniques entre Etats ou prestataires de services de certification électronique n'est pas encore mise en œuvre, sauf en vertu des dispositions sur la reconnaissance des certificats étrangers dans le cadre de la Communauté européenne en vertu de la directive 1999/93 (article 7 de la directive)[39] ; et que les « accords de certification croisée entre prestataires de services de certification électronique n'existent pas encore »[40]. Il convient donc de vérifier si la signature et le certificat présentent un degré de fiabilité équivalent aux normes internationales pour déterminer si la signature électronique est qualifiée. Nous nous demandons aussi quel effet juridique aura une signature électronique qui ne répond aux critères susmentionnés ?

2.2. L'effet juridique d'une signature électronique non qualifiée

Nous pouvons déduire de ce qui a été mentionné précédemment qu'une signature électronique non qualifiée est une signature électronique qui n'est pas dotée d'un certificat de conformité et d'un certificat électronique délivrés par le prestataire de service de conformité électronique.

Avant la promulgation de la loi °43-20 relative aux services de confiance pour les transactions électroniques, la loi n°53-05 relative à l'échange électronique des données juridiques ne reconnaissait que la signature électronique sécurisée. Nous nous demandons alors si une signature électronique non sécurisée est une signature électronique non reconnue par la loi et par conséquent ne produit aucun effet juridique. La loi est restée silencieuse, elle n'a ni confirmé ni infirmé cette hypothèse. Nous pouvons alors nous référer à l'article 417 du dahir formant code des obligations et des contrats. En effet, un écrit électronique qui n'est pas

[36] Clifford Chance, « Utilisation de la signature électronique au Maroc », mai 2020.

[37] Article 22 du 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.

[38] Article 12 de la loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation, 2001

[39] E. CAPRIOLI, Droit international de l'économie numérique, Les problèmes liés à l'internationalisation de l'économie numérique, éd. LexisNexix, 2007, p. 87- 90.

[40] V. O. CACHARD, La régulation internationale du marché électronique, LGDJ 2002.

authentique peut-être considéré comme un écrit électronique sous seing privé, dans ce cas, si les parties n'ont pas défini la force probante, c'est à la juridiction de statuer sur cette question.

En décembre 2020, la promulgation de la loi °43-20 relative aux services de confiance pour les transactions électroniques a brisé le doute et a emmené une clarification sur ce point. Il a tout d'abord mentionné deux autres types de signatures électroniques à savoir la signature électronique simple et la signature électronique avancée. La signature électronique simple est « la signature qui consiste en 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 »[41]. La signature électronique avancée est une signature électronique simple qui est propre au signataire et permet de l'identifier ; dont l'utilisation est exclusive au signataire et qui permet à ce dernier de détecter toute modification ultérieure ; et qui repose sur un certificat électronique[42]. D'après cette définition, nous pouvons constater que la différence entre la signature électronique avancée et la signature électronique qualifiée est l'absence de la certification du dispositif de création de signature électronique dans la signature électronique avancée.

La loi n°43-20 relative aux services de confiance pour les transactions électroniques ne s'est pas arrêtée à apporter deux autres types de signatures électroniques. Elle a mentionné dans son article 7 que « l'effet juridique et la recevabilité d'une signature électronique simple ou avancée comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée ». En d'autres termes, bien qu'un acte contenant une signature électronique simple ou une signature électronique avancée ne soit pas reconnu comme un acte authentique, il peut produire des effets juridiques et être recevable comme preuve devant la justice marocaine. Ainsi, cette disposition débloque la limitation de l'utilisation d'une signature électronique dans le cadre des contrats internationaux car le Maroc a assoupli les règles existantes.

Conclusion

A la lumière de ce qui précède, nous pouvons dire que la signature électronique, de par les procédés techniques utilisés pour sa mise en place, peut être un moyen efficace pour vérifier l' « authenticité » et l' « intégrité » d'un écrit électronique et garantir sa « confidentialité ». A ce jour, le Maroc reconnaît l'existence de trois types de signatures électroniques : la signature électronique simple, la signature électronique avancée et la signature électronique qualifiée[43]. En général, une signature électronique garantit le lien entre l'acte et le signataire, est propre et exclusive au signataire, permet de l'identifier et lui permet de détecter toute modification

[41] Article 2 du 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.

[42] Article 5 du 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.

[43] Article 4 et suivants du 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.

ultérieure. La particularité de la signature électronique avancée est qu'elle est accompagnée d'un certificat électronique. Quant à la signature électronique qualifiée, elle est accompagnée d'un certificat de conformité et d'un certificat électronique. Pour qu'un écrit électronique ait la même force probante qu'un acte authentique, il faut que la signature électronique qui y est apposée soit qualifiée. Cependant, cela n'exclut pas la possibilité d'utilisation d'un autre type de signature électronique car même en n'étant pas qualifiée, une signature électronique peut produire des effets juridiques et être recevable devant une juridiction marocaine. En effet, la technique utilisée, à savoir la cryptographie est un excellent moyen pour vérifier l'identité du signataire, en plus, cette technologie offre une grande précision en termes d'horodatage de l'acte signé. Malgré tous les avantages de la signature électronique, son utilisation n'est pas encore vulgarisée. Nous pouvons constater une utilisation hybride entre la signature manuscrite et électronique. Par exemple pour les opérations bancaires à haute valeur ajoutée, comme les demandes de crédits immobiliers, les banques convoquent leurs clients sur place pour qu'ils signent manuscritement. L'hésitation de l'utilisation totale de la signature électronique est compréhensible car la migration totale vers celle-ci nécessiterait une réorganisation de leur fonctionnement en entier[44]. En outre, il est important de se référer au système législatif en place lors d'une signature, que ce soit une signature manuscrite ou électronique[45]. Au Maroc, la législation relative à la signature électronique est à jour, toutefois, nous nous demandons si elle est complète. Nous pouvons répondre à cette question et y remédier après plusieurs pratiques. Ne serait-il pas aussi intéressant d'analyser la sécurité des données personnelles dans le cadre de l'utilisation de la signature électronique ?

[44] Pascal Colin, « Les gains de productivité avec la signature électronique sont impressionnants », Docusign, Briefing technologies bancaires, avril 2016, p.12-13.

[45] V. E. CAPRIOU, signature et courrier électroniques en droit comparé, commentaire d'une décision anglaise : England and Wales High Court (Chancery Division) Decisions, 7 avril 2006, dec. Case N° : M5X152, (Nilesh Mehta c/ J. Pereira Fernandes SA) : Comm. com. électr. juin 2006, n°103, p. 43.

Bibliographie

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.

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

Arrêt de la Cour de cassation de Rabat n°9, dossier n°100/2/1/2005, en date du 04/01/2006.

Arrêt de la Cour de cassation de Rabat, dossier n° 737/5/1/2007, en date du 21/05/2018.

Arrêt de la Cour de cassation de Rabat, chambre sociale, n°244, dossier n°1442/5/1/2017, en date du 28/03/2018.

Arrêt de la Cour de Cassation de Rabat n°147, dossier n°858/5/1/2018, en date du 29/01/2019.

Arrêt de la Cour de Cassation de Rabat n°521, dossier n°2390/5/1/2016, en date du 05/05/2017.

E. CAPRIOLI, Droit international de l'économie numérique, Les problèmes liés à l'internationalisation de l'économie numérique, éd. LexisNexix, 2007, p. 87- 90.

ERAL-SCHUHL (Christiane), Cyberdroit - Le droit à l'épreuve de l'internet, collection Praxis Dalloz, 8ème édition Dalloz, 2020, 1888 p.

V. O. CACHARD, La régulation internationale du marché électronique, LGDJ 2002.

M. Bigarré, D. Leroy, L. Valat, Cryptographie : système RSA.

W. Diffie, P. Van Oorschot, M. Wiener, Authentication and authenticated key exchanges. Designs, Codes and Cryptography, juin 1992.

Mihir Bellare, Ran Canetti et Hugo Krawczyk, Keying, Hash Functions for Message Authentication, CRYPTO 1996, p. 1–15.

IZDI (Sana), La preuve du contrat électronique en droit marocain, Revue marocaine du droit commercial et des affaires, numéro double 4-5, 2018, p. 98 – 104.

V. E. CAPRIOU, signature et courrier électroniques en droit comparé, commentaire d'une décision anglaise : England and Wales High Court (Chancery Division) Decisions, 7 avril 2006, dec. Case N° : M5X152, (Nilesh Mehta c/ J. Pereira Fernandes SA) : Comm. com. électr. juin 2006, n°103, p. 43.

COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL (CNUDCI), Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques, Publicaiton des Nations Unies, Vienne, 2009.

Clifford Chance, Utilisation de la signature électronique au Maroc, mai 2020

Pascal Colin, Les gains de productivité avec la signature électronique sont impressionnants, Docusign, Briefing technologies bancaires, avril 2016, p.12-13.

Webographie

Site officiel Programme e-gouvernement Royaume du Maroc : http://www.egov.ma/fr/certification-%C3%A9lectronique , consulté le 10/08/2021 à 21h01.

Site Le portail du droit : https://www.droit.fr/definition/2081-force-probante/ , consulté le 22 juillet à 20h06.

L'informateur, Sécurité 5 : Signatures Digitales, https://www.youtube.com/watch?v=t3pzkDRgQW8&t=30s

L'informateur, Sécurité 6 : Protocoles Cryptographiques, https://www.youtube.com/watch?v=25HbXbccPUY&t=319s

https://elearning-facsci.univannaba.dz/pluginfile.php/13922/mod_resource/content/0/CHAP2.3_%20El%20Gamal.pdf , consulté le 26/07/2021 à 13h24.