International journal of applied management and economics
Vol : 02 , N° 13, Avril 2025
ISSN : 2509-0720

L'instauration de la confiance dans le contrat électronique : Cadre juridique et enjeux

Building confidence in electronic contract: legal framework and issues.

- **Auteur 1 :** BEL-AMIN Samir,
- **Auteur 2 :** EL MOUSTAINE Ismail,
- **Auteur 3 :** AZIOUAL Fadoua,
- **Auteur 4 :** LABZAE Oumaima,
- **Auteur 5 :** EL MORABIT Adnan,
- **Auteur 6 :** EL HADANI Kawtar,
- **Auteur 7 :** ASRI FENNASSI Nada,

(1) Enseignant-chercheur en Droit des Affaires, Faculté des sciences juridiques, économiques et sociales, Ain Sebâa, Université Hassan II, Casablanca, Maroc ;

(2) Doctorant en Droit privé, Faculté des sciences juridiques, économiques et sociales, Ain Sebâa, Université Hassan II, Casablanca, Maroc ;

(3) Doctorante en Droit privé, Faculté des sciences juridiques, économiques et sociales, Ain Sebâa, Université Hassan II, Casablanca, Maroc ;

(4) Doctorante en Droit privé, Faculté des sciences juridiques, économiques et sociales, Ain Sebâa, Université Hassan II, Casablanca, Maroc ;

(5) Doctorant en Droit privé, Faculté des sciences juridiques, économiques et sociales, Ain Sebâa, Université Hassan II, Casablanca, Maroc ;

(6) Doctorante en Droit privé, Faculté des sciences juridiques, économiques et sociales, Ain Sebâa, Université Hassan II, Casablanca, Maroc ;

(7) Doctorante en Droit privé, Faculté des sciences juridiques, économiques et sociales, Ain Sebâa, Université Hassan II, Casablanca, Maroc.

Conflit d'intérêt : L'auteur ne signale aucun conflit d'intérêt.

Pour citer cet article : BEL-AMIN .S, EL MOUSTAINE .I, AZIOUAL .F, LABZAE .O, EL MORABIT .A, EL HADANI .K & ASRI FENNASSI .N (2025) « L'instauration de la confiance dans le contrat électronique : Cadre juridique et enjeux »,

IJAME : Volume 02, N° 13 | Pp: 060 – 089.

Date de soumission : Mars 2025
Date de publication : Avril 2025

DOI : 10.5281/zenodo.15090677

Résumé

La problématique de la confiance aux contrats électroniques est apparue suite au développement d'internet et de moyens de communication, qui ont redéfini les critères de la confiance. Ce qui nécessite la mise en œuvre des fondements juridiques de confiance, en prenant en considération les défis qui en découlent, afin d'atteindre les résultats escomptés.

Ainsi, la confiance dans la formation des contrats électroniques s'articule autour de deux fondements, à savoir, le formalisme contractuel visant à clarifier les exigences de validité des contrats numériques, et les mécanismes de confiance mis en place qui s'articule autour de la signature électronique qui garantit l'authenticité et l'identité des signataires. C'est ainsi, et en s'appuyant sur la loi 43-20, que cet article propose des pistes d'amélioration en comparant le cadre juridique marocain avec celui de la France.

En parallèle, les enjeux de confiance dans l'exécution des contrats électroniques, revêt l'importance du respect des obligations contractuelles issues des contrats électroniques, tout en répondant aux défis de cybersécurité et de protection du consommateur, afin de garantir la sécurité des transactions.

C'est dans ce sens que notre article s'inscrit dans la perspective de joindre des notions fondamentales du droit qui ont connus une véritable refonte avec l'avènement des nouvelles technologies.

Mots clés : la signature électronique, cybercommerçant, cyberacheteur, la confiance, la certification des services électroniques.

Summary

The issue of trust in electronic contracts has arisen as a result of the development of the Internet and other means of communication, which have redefined the criteria for trust. This calls for the implementation of the legal foundations of trust, taking into account the challenges involved, in order to achieve the desired results.

Trust in the formation of electronic contracts hinges on two foundations, namely contractual formalism aimed at clarifying the validity requirements of digital contracts, and the trust mechanisms put in place, which revolve around the electronic signature that guarantees the authenticity and identity of the signatories. Based on Law 43-20, this article proposes ways of improving the Moroccan legal framework by comparing it with that of France.

At the same time, the challenges of trust in the performance of electronic contracts highlight the importance of compliance with contractual obligations arising from electronic contracts, while meeting the challenges of cybersecurity and consumer protection, in order to guarantee the security of transactions.

It is with this in mind that our article aims to bring together fundamental legal concepts that have undergone a veritable overhaul with the advent of new technologies.

Keywords: Electronic Signature, E-Merchant, E-Buyer, Confidence, Certification Of Electronic Services.

1. Introduction

L'essor des technologies numériques a fait du contrat électronique un élément clé du commerce moderne, facilitant les échanges et optimisant les processus juridiques. Au Maroc, cette évolution s'inscrit dans une stratégie nationale de digitalisation visant à moderniser l'économie et à renforcer sa compétitivité internationale, en s'alignant sur des normes mondiales comme le RGPD. Toutefois, cette transition requiert des mécanismes juridiques et techniques solides pour instaurer la confiance dans un environnement numérique où les interactions ne sont pas physiques.

La confiance dans les transactions numériques repose sur un environnement sécurisé garantissant l'intégrité, l'authenticité et la confidentialité des échanges, grâce à des mécanismes comme la certification des prestataires, la reconnaissance des signatures électroniques et des obligations strictes en matière de transparence et de sécurité des données. Malgré ces avancées, des obstacles subsistent : la méconnaissance des outils numériques par de nombreux acteurs, les risques de cyberattaques et les défis des consommateurs liés à la vie privée et à l'accès équitable aux services. Ces enjeux appellent à renforcer la sensibilisation et à établir un cadre juridique et technique conciliant innovation, sécurité et principes contractuels fondamentaux.

La confiance dans le contrat électronique repose sur un cadre juridique en constante évolution, tant au Maroc qu'en France. Au Maroc, la loi n° 53-05 reconnaît la signature électronique comme équivalente à la signature manuscrite, à condition d'utiliser un certificat délivré par un prestataire agréé. Ce cadre est renforcé par le Code des obligations et des contrats, ainsi que par des lois comme la loi n° 31-08 pour la protection des consommateurs, la loi n° 09-08 sur la protection des données personnelles, et la loi n° 05-20 sur la cybersécurité. En France, les contrats électroniques sont régis par le Code civil, la Loi pour la Confiance dans l'Économie Numérique (LCEN) et le règlement européen eIDAS, qui sécurise les échanges transfrontaliers. Le RGPD complète ce cadre en protégeant les données personnelles. Ces textes visent à garantir la fiabilité, la sécurité et la protection des parties dans les transactions électroniques.

Le cadre législatif marocain est complété par des décrets, notamment le décret n° 2-16-410 concernant l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), visant à renforcer la cybersécurité et protéger les utilisateurs. Le décret n° 2-13-881 du 28 rabii I 1436 (20 janvier 2015) modifie et complète le décret n° 2-08-518 du 25 joumada I 1430 (21 mai 2009), relatif à l'application de la loi n° 53-05 sur l'échange électronique des données juridiques. De plus, l'arrêté n° 3-74-11 fixe l'organisation de la direction générale de la sécurité des systèmes d'information, tandis que la circulaire du chef du gouvernement n° 2/2023 du 12

janvier 2023 s'applique à la directive nationale de la sécurité des systèmes d'information (SSI). L'ensemble de ce corpus normatif encadre les contrats électroniques en renforçant la sécurité et la fiabilité des transactions électroniques tout en protégeant les droits des utilisateurs.

L'étude des fondements de la confiance dans la formation et l'exécution des contrats électroniques permet d'approfondir la compréhension des évolutions juridiques face à la digitalisation des transactions commerciales. Théoriquement, cette analyse éclaire le rôle du formalisme contractuel dans un environnement numérique, en confrontant les conditions de validité du contrat électronique aux obstacles spécifiques qu'il rencontre, tels que la question de l'identification des parties et de la préservation de la volonté contractuelle. L'exploration des mécanismes de confiance, notamment à travers la e-signature et la certification des prestataires de services de confiance, propose un cadre théorique solide pour étudier comment ces outils garantissent la sécurité et l'intégrité des transactions électroniques. D'autre part, la réflexion sur les obligations respectives des parties contractantes et les défis liés à l'exécution du contrat électronique, comme les problèmes liés à la cybersécurité, souligne les enjeux théoriques d'une régulation adaptée pour un commerce numérique sécurisé. Ces approches offrent ainsi une base théorique essentielle pour comprendre les défis juridiques de la numérisation du droit des contrats.

D'un point de vue pratique, cette étude revêt une importance capitale pour les acteurs du commerce électronique, les prestataires de services de confiance, ainsi que les législateurs et régulateurs. Les mécanismes de confiance étudiés, comme la e-signature et la certification des prestataires, sont des outils concrets pour renforcer la sécurité des transactions en ligne, apportant une garantie d'authenticité et de non-répudiation des actes juridiques. La prise en compte des obligations spécifiques des cybercommerçants et des cyberacheteurs est indispensable pour assurer la bonne exécution des contrats, prévenir les litiges, et renforcer la confiance des consommateurs dans l'e-commerce. En outre, les défis liés à la cybersécurité, notamment les risques de fraude et de piratage, mettent en lumière la nécessité d'un cadre juridique et technique robuste pour protéger les données personnelles et assurer la sécurité des transactions. Ainsi, l'intérêt pratique de cette analyse réside dans sa capacité à fournir des solutions concrètes aux problèmes quotidiens rencontrés dans le domaine du commerce électronique, en renforçant la fiabilité et la transparence des relations contractuelles en ligne.

Cette double dimension théorique et pratique nous mène à poser la problématique suivante : Dans quelle mesure est-il possible d'instaurer une confiance durable et sécurisée dans les contrats électroniques en relevant les défis liés à l'authentification des parties, à la certification

des prestataires de services de confiance et à la cybersécurité, tout en s'appuyant sur les avancées juridiques et technologiques pour garantir la protection des données sensibles et le respect des obligations des parties prenantes ?

Afin de répondre à cette problématique et d'évaluer l'efficacité de l'instauration des fondements de confiance dans les contrats électroniques, nous optons une approche juridique et analytique, fusionnant une analyse comparative et une étude normative. Cette méthodologie de recherche se fonde sur plusieurs fondements d'évaluation : les fondements de la confiance, les enjeux techniques et juridiques, l'authenticité de la signature électronique, la protection du consommateur dans les contrats électroniques, et la conformité aux règles juridiques nationaux et internationaux.

L'analyse de cet article s'articule en deux parties. La première partie analyse les fondements de la confiance dans la formation du contrat électronique (2), en étudiant les conditions de validité, les obstacles à sa formation, et les mécanismes d'authentification comme la signature électronique. La seconde partie examine les enjeux de la confiance dans l'exécution du contrat électronique (3), en se concentrant sur les obligations des parties contractantes et les défis liés à la cybersécurité et à la protection des consommateurs.

2. Les fondements de la confiance dans la formation du contrat électronique

La transformation numérique a profondément modifié les interactions économiques et juridiques, faisant du contrat électronique une composante incontournable des échanges modernes. Cette reconnaissance en tant que forme juridique légitime a imposé une révision des règles classiques relatives à la formation et à l'exécution des contrats.

Bien que reposant sur les mêmes principes fondamentaux que les contrats traditionnels, le contrat électronique se distingue par son caractère dématérialisé, ce qui engendre des enjeux spécifiques en matière de formalisme et de confiance.

Ainsi, la formation du contrat électronique exige une adaptation des règles traditionnelles liées à l'offre, à l'acceptation et à la rencontre des volontés, afin de garantir la validité et la protection des parties (2.1). De plus, la confiance et la sécurité juridique des échanges reposent sur des mécanismes de validation et de sécurisation des données, tels que la signature électronique et les systèmes de certification, assurant l'intégrité et l'authenticité des transactions numériques (2.2).

2.1 Le formalisme contractuel à l'épreuve du contrat électronique

La transformation numérique a redéfini les modes de contractualisation, faisant du contrat électronique un pilier des échanges commerciaux modernes. Ce bouleversement impose une

adaptation des notions d'écrit, de signature, de consentement, et des mécanismes d'offre et d'acceptation, afin de garantir sécurité juridique et conformité au contexte numérique.

Au Maroc, les contrats électroniques sont encadrés par les lois n° 53-05 et n° 43-20, tandis qu'en France, ils reposent sur le Code civil, la loi LCEN et le règlement eIDAS. Si ces cadres garantissent leur validité et leur sécurité, leur mise en œuvre pratique pose des défis, notamment en matière d'interprétation des principes juridiques dans un environnement numérique évolutif. Ce chapitre examinera, d'une part, les conditions de validité des contrats électroniques (2.1.1) et, d'autre part, les obstacles à leur formation (2.1.2).

2.1.1 Les conditions de validité du contrat électronique

La formation d'un contrat, qu'il soit traditionnel ou électronique, repose sur des conditions de validité essentielles. Certaines sont similaires à celles d'un contrat classique, tandis que d'autres sont adaptées au numérique. En droit marocain, ces conditions, énumérées à l'article 2 du DOC, comprennent la capacité, le consentement non vicié, un objet certain et une cause licite. En droit français, elles se limitent à trois : la capacité, le consentement libre et éclairé, ainsi qu'un objet licite et certain, selon l'article 1128 du Code civil. Bien que ces principes s'appliquent également aux contrats électroniques, ces derniers nécessitent des adaptations spécifiques, notamment pour l'écrit (i), la signature électronique (ii), le consentement des parties (iii) et les mécanismes d'offre et d'acceptation (iiii).

i L'écrit électronique et son équivalence

L'émergence de l'écrit électronique, favorisée par la révolution numérique et la mondialisation des échanges, a abouti à sa reconnaissance comme mode de preuve équivalent à l'écrit papier. En droit marocain, cette équivalence est consacrée par l'article 417-1 du Dahir des Obligations et des Contrats (DOC), modifié par la loi n° 53-05. Elle repose sur deux conditions cumulatives fondamentales qui sont l'identification claire de l'auteur et la garantie de l'intégrité et de la conservation du document. En droit français, cette reconnaissance, soumise aux mêmes conditions est prévue à l'article 1366 du Code civil.

Contrairement à l'écrit papier, l'écrit électronique se distingue par sa dématérialisation, sa traçabilité et sa durabilité grâce aux technologies numériques. Cependant, ces avantages imposent des contraintes techniques pour garantir sa fiabilité. Ainsi, des outils tels que les certificats électroniques, les systèmes de cryptage et les technologies d'horodatage assurent l'identification de l'auteur, la détection d'éventuelles altérations et la conservation durable des documents. Pour être juridiquement valable, l'écrit électronique doit satisfaire trois critères. Tout d'abord, il doit revêtir d'un critère identifiable, permettant de remonter de manière fiable

à l'auteur, notamment grâce à des certificats numériques. Ensuite, il doit garantir l'intégrité de l'écrit en détectant toute modification ou altération assurant sa conformité à l'original. Enfin, il doit répondre aux exigences de conservation en garantissant la lisibilité et l'accès durable au document, comme l'exige l'article 440 du DOC ((Modifié par l'article 5 de la loi n° 53-05).

En adoptant les normes internationales de la Commission des Nations Unies pour le droit commercial international (CNUDCI), le cadre marocain s'aligne sur le principe d'équivalence fonctionnelle, qui garantit la validité juridique des écrits électroniques. Néanmoins, leur application pratique demeure conditionnée par des technologies robustes, la protection contre les falsifications et une gestion documentaire sécurisée. En définitive, l'écrit électronique représente une avancée significative, mais son efficacité juridique repose sur des solutions techniques fiables et une vigilance accrue face aux défis de la cybersécurité et de la conservation des données.

ii La signature électronique comme garantie de validité

La signature électronique joue un rôle fondamental dans la formation des contrats électroniques, car elle constitue un élément clé pour garantir leur validité. Elle remplit plusieurs fonctions essentielles : authentifier l'auteur de l'acte, manifester son consentement et préserver l'intégrité du document signé. Elle figure à l'article 417-3 du Dahir des Obligations et des Contrats (DOC) en droit marocain et à l'article 1367 du Code civil en droit français.

Pour être considérée valide, la signature électronique doit répondre à certaines conditions : elle doit permettre une identification fiable de son auteur et garantir que le contenu du document n'a pas été altéré après sa signature. En outre, une distinction est opérée entre la signature électronique ordinaire, admise à titre de preuve, et la signature électronique sécurisée, qui bénéficie d'une présomption légale de fiabilité lorsqu'elle est apposée via un certificat délivré par une autorité de certification agréée.

La reconnaissance de la signature électronique dans le cadre juridique marocain s'aligne sur les standards internationaux et témoigne d'une volonté de renforcer la confiance dans les transactions numériques, tout en assurant la sécurité juridique des parties contractantes. Ce mécanisme sera abordé de manière plus approfondie dans le chapitre suivant, notamment en ce qui concerne son rôle en tant que moyen d'authentification et l'importance des prestataires de services de confiance.

iii Le consentement dans l'environnement électronique

Le consentement, élément central de la formation contractuelle, prend une dimension particulière dans l'environnement numérique. La dématérialisation des échanges remplace les

interactions physiques et les signatures manuscrites par des mécanismes numériques tels que le clic d'approbation, la signature électronique ou la validation en ligne, tout en respectant les principes de liberté, d'éclairage et d'intention manifeste.

En France, le consentement électronique, reconnu par l'article 1367 du Code civil, se matérialise souvent par un clic. Une procédure de double clic, courante, permet de choisir un produit ou service avant de confirmer l'intention d'achat. L'acceptation des conditions générales de vente (CGV), qui encadrent les délais de livraison, les garanties et le droit de rétractation, est également obligatoire. L'article L221-5 du Code de la consommation impose que ces CGV soient accessibles avant la conclusion du contrat.

Au Maroc, l'article 3 de la loi n° 53-05 impose également la mise à disposition et l'acceptation des CGV avant la formation du contrat. Conformément au principe d'équivalence fonctionnelle, cette loi confère à l'offre et à l'acceptation électroniques la même valeur juridique que leurs formes classiques, sous réserve de garantir l'identité des parties et l'intégrité des documents. L'article 417-1 du DOC renforce cette équivalence en accordant à l'écrit électronique la même force probante que l'écrit papier, sous condition d'une conservation fiable.

La traçabilité et la preuve du consentement reposent sur des outils tels que l'horodatage, les certificats numériques et les journaux électroniques. Pour être valable, le consentement électronique doit rester libre, éclairé et exempt de vices, conformément à l'article 1128 du Code civil français.

Cependant, bien que le consentement électronique constitue une pierre angulaire de la formation contractuelle, il ne suffit pas à lui seul. Les mécanismes d'offre et d'acceptation adaptés au numérique assurent également la validité et la traçabilité des contrats électroniques.

iiii L'offre et l'acceptation dans les transactions électroniques

L'offre et l'acceptation, fondements de la formation contractuelle, prennent une dimension particulière dans les transactions électroniques, où leur exécution est dématérialisée. L'article 65-5 du DOC, applique la théorie de la réception en stipulant que le contrat électronique est formé dès que l'acceptation parvient à l'offrant, sauf stipulation contraire. Cette disposition transpose les principes classiques du droit des contrats à l'environnement numérique tout en tenant compte de ses spécificités techniques.

Cependant, des défis techniques subsistent, notamment les interruptions, erreurs ou délais dans les transmissions électroniques, qui peuvent compromettre la réception de l'acceptation et la formation du contrat. L'absence de mécanismes comme la confirmation de réception sur certaines plateformes numériques aggrave ces incertitudes, augmentant les risques de litiges.

Pour renforcer la sécurité des transactions électroniques, des outils tels que les accusés de réception électroniques et les technologies d'horodatage sont essentiels pour garantir la traçabilité et offrir des garanties probatoires solides en cas de contestation. Par ailleurs, l'adoption de normes internationales, comme le règlement eIDAS, pourrait inspirer le cadre juridique marocain, notamment pour améliorer la confiance des contrats électroniques et encourager les échanges transfrontaliers.

En somme, si l'article 65-5 du DOC offre une base juridique robuste, des ajustements pratiques sont nécessaires pour répondre aux défis spécifiques du numérique. L'intégration de mécanismes de confirmation et de standards internationaux reste essentielle pour renforcer la confiance et protéger les parties contractantes dans l'environnement numérique.

2.1.2 Les obstacles à la formation du contrat électronique

Malgré les avancées juridiques et technologiques, la formation des contrats électroniques demeure confrontée à de nombreux défis. Ces obstacles, qu'ils soient techniques, juridiques ou sociétaux, affectent des aspects fondamentaux tels que le consentement, la transparence et la sécurité des transactions.

D'une part, les limites liées au consentement et à l'exclusion numérique restreignent l'accès équitable aux outils numériques (i), compromettant ainsi la clarté et l'équilibre des engagements. D'autre part, les obstacles techniques et juridiques posent des questions cruciales quant à la fiabilité et à la sécurité des transactions électroniques (ii).

i Les défis liés au consentement et à la fracture numérique

La formation du contrat électronique est particulièrement affectée par la fracture numérique, qui prive une partie importante de la population de l'accès aux outils nécessaires à la contractualisation en ligne. Cette fracture résulte de disparités économiques et géographiques, limitant la capacité de certaines personnes à interagir avec les systèmes numériques. Par conséquent, cette inégalité pose des défis en matière d'inclusivité, empêchant certains individus d'exprimer un consentement libre et éclairé. Cette situation est encore exacerbée dans les régions où les infrastructures technologiques sont insuffisantes ou absentes.

Le consentement électronique, bien qu'encadré par des lois au Maroc, soulève des défis propres à l'environnement numérique. Les pratiques courantes telles que l'acceptation par un simple clic ou la validation en ligne, combinées à des conditions générales longues et complexes, peuvent compromettre la qualité du consentement. Ces dernières ne sont souvent ni pleinement lues ni comprises par les utilisateurs, entraînant des engagements contractuels peu éclairés. Par ailleurs, des pratiques abusives, telles que les interfaces manipulatives (aussi appelées "dark

patterns"), influencent de manière biaisée les choix des utilisateurs, compromettant la liberté de leur engagement. Ces défis remettent en question la transparence et l'équité des contrats électroniques.

ii Les défis techniques et juridiques des contrats électroniques

Les défis techniques jouent également un rôle crucial dans les obstacles à la formation des contrats électroniques. Les interruptions de service, les erreurs de transmission et les cyberattaques sont autant de facteurs pouvant perturber l'expression et la réception du consentement, de l'offre ou de l'acceptation. Ces vulnérabilités compromettent la fiabilité et l'intégrité des transactions numériques. De plus, l'absence d'interopérabilité entre différentes plateformes ou systèmes complique la conclusion des contrats, entraînant des retards ou des dysfonctionnements.

Sur le plan juridique, les règles traditionnelles du droit des obligations sont parfois difficiles à appliquer dans un cadre numérique. La preuve du consentement repose souvent sur des outils techniques comme l'horodatage ou les certificats électroniques. Bien que ces outils offrent une certaine traçabilité, ils ne garantissent pas toujours une fiabilité absolue, en particulier en cas de litige ou de manipulation. Les menaces en matière de cybersécurité aggravent ces défis. La manipulation des données, l'usurpation d'identité ou encore le piratage des signatures électroniques remettent en cause l'authenticité et l'intégrité des contrats électroniques. Ces risques technologiques, s'ils ne sont pas maîtrisés, érodent la confiance des parties dans les échanges numériques. Enfin, la transparence contractuelle constitue un autre obstacle majeur. L'asymétrie d'informations entre les parties, notamment entre les consommateurs et les grandes plateformes numériques, crée un déséquilibre contractuel. Les termes contractuels opaques et complexes renforcent cette vulnérabilité, remettant en cause la liberté et la compréhension du consentement.

La complexité croissante des transactions électroniques nécessite des réponses adaptées, combinant inclusion numérique et harmonisation des cadres juridiques à l'échelle internationale. Cependant, au-delà de ces solutions globales, un autre aspect fondamental émerge : la consolidation de la confiance, qui est un pilier incontournable de la sécurité juridique des contrats électroniques. En effet, cette confiance repose sur des mécanismes spécifiques, tels que la signature électronique et la certification des prestataires, qui assurent l'authenticité et l'intégrité des échanges dans un environnement numérique. C'est précisément sur ces dispositifs que se concentrera le chapitre suivant.

2.2 Les mécanismes de confiance dans le contrat électronique

La transition numérique, marquée par des avancées majeures comme le big data, les algorithmes prédictifs, l'intelligence artificielle et l'informatique quantique, a profondément transformé les échanges juridiques et économiques. Ces évolutions ont bouleversé le pilier central de la confiance, exigeant son adaptation aux défis de la dématérialisation et des technologies numériques.

Traditionnellement incarnée par l'écrit et la signature manuscrite, la confiance s'est redéfinie à travers des mécanismes modernes répondant aux spécificités de l'ère numérique. Ces transformations ont introduit des outils tels que la signature électronique, devenue une réponse incontournable pour garantir l'intégrité et l'authenticité des transactions dans un environnement dématérialisé.

Au Maroc, la signature électronique bénéficie d'un cadre juridique rigoureux qui lui confère une véritable force probante, sous certaines conditions (2.1). Soutenue par des dispositifs de certification et des normes internationales, elle constitue bien plus qu'un simple outil technique : elle est aujourd'hui un fondement essentiel de la sécurité juridique et de la confiance dans les contrats électroniques (2.2). Ces mécanismes modernes jouent un rôle clé dans la consolidation des échanges numériques, en assurant à la fois leur validité et leur fiabilité.

2.2.1 La e-signature comme moyen d'authentification dans le contrat électronique

La question de la valeur de l'écrit numérique par rapport à celui manuscrit n'est plus d'actualité. En effet, il est désormais reconnu qu'un écrit électronique a la même force probante qu'un écrit sur papier. Cette reconnaissance repose sur un fondement essentiel qui est l'adossement d'une signature électronique ou e-signature, à l'écrit numérique.

La signature électronique désigne un ensemble de données électroniques jointes ou associées à un message électronique (2.1.1), permettant d'identifier le signataire et d'exprimer son consentement. Cette définition large englobe toutes les formes de signatures électroniques, des plus simples aux plus sophistiquées (2.1.2). Ceci explique son adoption massive dans les transactions numériques, notamment dans la finance, le commerce électronique et les marchés publics.

2.2.2 La signature électronique sécurisée : une garantie d'authenticité

En droit marocain, la signature électronique est encadrée par la loi n° 53-05 relative à l'échange électronique de données juridiques. L'article 8 de cette loi définit les conditions techniques et juridiques nécessaires pour garantir la validité et la sécurité de ce dispositif, en s'appuyant sur des technologies de cryptographie asymétrique. Ce choix témoigne d'une volonté d'assurer un

haut niveau de sécurité et d'authenticité dans les transactions numériques. La signature électronique sécurisée repose sur un système de cryptographie asymétrique, qui garantit la confidentialité et l'intégrité des données. Ce procédé, basé sur deux clés complémentaires, permet à la clé publique de chiffrer les données et à la clé privée, détenue exclusivement par le signataire, de les déchiffrer. Cette technologie offre une protection efficace contre toute tentative d'usurpation ou d'altération, en rendant impossible la déduction de la clé privée à partir de la clé publique.

Pour être valide en droit marocain, une signature électronique doit répondre à plusieurs exigences fondamentales. Elle doit d'abord permettre l'identification fiable du signataire, établissant ainsi un lien indéniable entre l'auteur et l'acte signé. Ensuite, elle doit être générée par des moyens que le signataire contrôle exclusivement, afin de prévenir toute utilisation frauduleuse. Enfin, la signature doit garantir un lien indissociable avec le document auquel elle est apposée, de manière à détecter toute modification ultérieure.

Ces critères visent à assurer deux propriétés essentielles : l'authenticité et l'intégrité. L'authenticité consiste à établir avec certitude l'identité de l'expéditeur, tandis que l'intégrité garantit que le contenu du document reste inchangé depuis sa signature. Par conséquent, une signature électronique sécurisée confère aux échanges numériques une fiabilité comparable, voire supérieure, à celle des signatures manuscrites dans les transactions traditionnelles.

La signature électronique joue ainsi un rôle crucial dans la préservation de la confiance dans un environnement numérique. En répondant aux exigences techniques et juridiques strictes, elle assure que les documents signés numériquement soient non seulement conformes à la loi, mais également dignes de confiance pour toutes les parties concernées.

2.2.3 Les différents types de signature électronique

Le cadre juridique marocain a été enrichi par la loi n° 43-20, qui introduit une classification des signatures électroniques en trois catégories : simple, avancée, et qualifiée. Cette classification s'aligne sur le droit français, où elle est régie par le règlement européen eIDAS, témoignant ainsi d'une convergence des normes internationales en matière de transactions numériques.

La signature électronique simple, définie à l'article 2 de la loi n° 43-20, repose sur un procédé fiable d'identification électronique garantissant le lien avec l'acte signé et exprimant le consentement du signataire. Cette forme est souvent matérialisée par des codes confidentiels ou des mots de passe, utilisés dans des transactions à faible enjeu, telles que la validation d'un formulaire numérique ou la confirmation d'un abonnement en ligne. En France, cette catégorie de signature est également reconnue mais limitée à des usages où les risques de falsification

sont faibles.

La signature électronique avancée constitue un niveau supérieur de sécurité. En droit marocain, elle permet une identification claire du signataire et garantit l'intégrité du document, empêchant toute modification après signature. Elle repose sur des technologies telles que les certificats électroniques ou les signatures biométriques, qui renforcent sa fiabilité. Cette classification existe également en droit français, où elle répond aux mêmes exigences techniques, notamment l'utilisation de données cryptographiques sous le contrôle exclusif du signataire.

Enfin, la signature électronique qualifiée représente la forme la plus sécurisée et juridiquement contraignante. En droit marocain, comme en droit français, elle repose sur l'utilisation de dispositifs qualifiés et de certificats délivrés par des prestataires de confiance agréés, conformes à des normes strictes. L'article 6 de la loi n° 43-20 précise que cette signature est équivalente à une signature manuscrite, offrant les garanties les plus élevées en termes d'authenticité, d'intégrité, et d'identification du signataire. Le règlement eIDAS en France adopte une approche similaire, en exigeant une validation rigoureuse par des autorités certifiées.

Cette convergence entre le cadre marocain et le cadre européen démontre une volonté commune d'adapter le niveau de sécurité des signatures électroniques aux enjeux des transactions numériques, tout en facilitant leur reconnaissance mutuelle dans un contexte international.

L'existence de différentes formes de signatures électroniques de la simple à la qualifiée illustre leur adaptabilité à des contextes variés. Elles répondent aussi bien à des besoins courants, où les risques sont limités, qu'à des situations complexes et sensibles, nécessitant un haut niveau de sécurité. Cependant, cette accessibilité accrue s'accompagne de nouveaux risques, tels que les usurpations d'identité ou la falsification des signatures. Face à ces défis, le législateur a prévu l'intervention de tiers de confiance, désignés juridiquement comme prestataires de services de certification électronique, afin de sécuriser les échanges numériques et protéger les utilisateurs.

2.3 La certification des prestataires de services de certification électronique

La certification des prestataires de services de confiance est essentielle pour sécuriser les signatures électroniques et garantir leur conformité aux normes internationales. Ces prestataires, véritables tiers de confiance, jouent un rôle clé en renforçant l'authenticité et l'intégrité des transactions numériques (2.2.1). Au Maroc, ce système repose sur un cadre légal rigoureux, mais présente certaines limites dans son application internationale. Une comparaison avec le modèle français permet d'éclairer les défis et les opportunités pour améliorer ce mécanisme (2.2.2).

2.3.1 Le rôle des prestataires de certification électronique

Les prestataires de services de certification électronique occupent une place centrale dans l'écosystème des transactions numériques. Au Maroc, ces prestataires, qui doivent obligatoirement avoir leur siège dans le pays, sont agréés et contrôlés par l'autorité nationale d'agrément et de surveillance de la certification électronique. Leur mission consiste principalement à délivrer des certificats électroniques qualifiés et à garantir leur conformité avec les normes internationales, en assurant à la fois la sécurité et l'authenticité des signatures électroniques.

Une signature électronique qualifiée ne peut être valide qu'après l'obtention d'un certificat de conformité délivré par l'autorité compétente. Ce certificat assure la confidentialité, l'intégrité et l'unicité des données de création des signatures électroniques. Il offre également une protection contre les usages frauduleux, y compris ceux provenant de parties étrangères. En vertu du principe de non-discrimination énoncé dans l'article 12 de la loi type de la CNUDCI, un certificat étranger peut être reconnu au Maroc, à condition qu'il respecte les standards internationaux et qu'un accord bilatéral ou multilatéral ait été conclu entre les parties concernées.

En pratique, au Maroc, Barid eSign est la seule plateforme habilitée à délivrer des certificats électroniques qualifiés. Ce monopole garantit la force probante des signatures électroniques pour les transactions nationales. Cependant, cette exclusivité présente des limites, notamment dans un contexte international, où l'utilisation des signatures électroniques marocaines reste restreinte. De plus, l'obtention d'un certificat qualifié nécessite une présence physique au Maroc, ce qui constitue une contrainte pour les citoyens marocains résidant à l'étranger.

Un exemple de l'efficacité de ce système est observé dans le secteur notarial. Après la crise sanitaire du Covid-19, les notaires marocains ont pu moderniser leurs pratiques grâce à la plateforme Tawtik, intégrant l'extension Barid eSign. Ce système leur permet d'apposer divers types de sceaux électroniques, comme des sceaux d'original ou de copie conforme, renforçant ainsi la sécurité et la fiabilité des actes notariés.

2.3.2 Comparaison avec le cadre français

Contrairement au Maroc, où un monopole est en place, la France offre une pluralité de prestataires de certification électronique inscrits sur la Trusted List européenne, supervisée par l'ANSSI. Des acteurs tels que ChamberSign France, Certinomis et DocuSign proposent des solutions variées, répondant aux besoins des particuliers comme des entreprises.

Une différence majeure réside dans la procédure de vérification d'identité. En France, cette

vérification peut être réalisée à distance grâce à des technologies innovantes, telles que les solutions vidéo ou les systèmes biométriques. Ce processus simplifié favorise une adoption rapide et large des signatures électroniques qualifiées, tout en maintenant un haut niveau de sécurité.

Ce cadre flexible contraste avec le système marocain, principalement orienté vers des usages institutionnels et professionnels. Bien que le cadre marocain repose sur des bases solides et garantisse une sécurité élevée, il reste conçu pour des transactions locales, limitant son interopérabilité et son accessibilité à l'échelle internationale. Dans un contexte global, où l'harmonisation et la reconnaissance mutuelle des certificats électroniques sont essentielles, des évolutions deviennent nécessaires.

En vertu de l'article 12 de la loi type de la CNUDCI, qui promeut le principe de non-discrimination, le Maroc pourrait renforcer ses accords bilatéraux ou multilatéraux pour élargir la reconnaissance des certificats étrangers. Par ailleurs, l'intégration de technologies permettant une vérification d'identité à distance élargirait l'accès aux services de certification, notamment pour les citoyens marocains résidant à l'étranger. Enfin, l'ouverture à une pluralité de prestataires renforcerait la diversité et la compétitivité du secteur, rendant ces services plus accessibles au grand public.

En s'inspirant du modèle français, qui allie flexibilité et accessibilité grâce à la diversité de ses prestataires, le Maroc pourrait adapter son système pour démocratiser l'usage des signatures électroniques. Cette évolution permettrait non seulement de répondre aux besoins croissants des utilisateurs, mais également d'accroître l'attractivité des transactions numériques marocaines dans un environnement globalisé.

3. Les enjeux de la confiance dans l'exécution du contrat électronique

La consécration de la confiance dans l'exécution des contrats électroniques est un objectif qui nécessite la prise en considération de plusieurs enjeux. Certes, la force probante des contrats électroniques est identique à celle des contrats classiques, mais la vocation électronique produit une relation juridique à caractère numérique. Ces contrats mettent en liaison juridique deux parties contractantes, en l'occurrence le cyber commerçant en tant que vendeur d'une chose ou d'un service, et le cyber acheteur en tant que consommateur. Le recours aux contrats électroniques facilite les transactions commerciales, et favorise le développement économique. Mais cette forme électronique nous amène à mettre en exergue plusieurs enjeux.

D'abord, l'exécution des contrats électroniques met à la charge des deux parties contractantes des obligations à respecter. Le respect de ces obligations contractuelles concrétise la confiance

à ces contrats électroniques (3.1). D'autre part des enjeux d'exécution de ces contrats se présentent et doivent être pris en considération afin de renforcer le caractère de confiance (3.2).

3.1 Les obligations des parties contractantes

L'exécution des contrats électroniques produit un engagement issu d'un échange électronique, qui doit être respecté par les parties contractantes. La bonne exécution du contrat électronique est l'un des enjeux de confiance de ces contrats. C'est pour cette raison, qu'il nous parait crucial de mettre en évidence les obligations d'exécution à respecter par le cyber commerçant d'une part (3.1.1), ainsi que par le cyber acheteur d'autre part (3.1.2).

3.1.1 Les obligations du cyber commerçant

Dans le cadre des contrats électroniques, le cyber commerçant est tenu d'honorer à ses engagements contractuels, et de respecter ses obligations pour assurer une bonne exécution, et de maintenir une confiance entre les parties contractantes, ainsi que toute personne désirant de recourir auxdits contrats.

Le cyber commerçant est un auteur de l'offre de la vente électronique. Il est tenu donc avant d'exécuter le contrat, de recevoir un accusé de réception de l'offre, ainsi que l'acceptation du cyber acheteur, pour que la commande électronique soit confirmée. Après sa confirmation, le cyber commerçant en tant que vendeur exécute le contrat électronique par : la délivrance de la chose dans le délai imparti (i), ainsi que la garantie de la chose objet du contrat (ii).

i La délivrance de la chose objet du contrat

Le cyber commerçant doit veiller à la délivrance de la chose objet du contrat électronique dans les délais impartis. A cet effet, l'article 12 de la loi 31-08 relative à la protection du consommateur précise que lorsque le prix convenu excède un seuil légal de 3 000 dirhams, et que la livraison n'est pas faite immédiatement, il faut préciser dans le contrat électronique établi, la date limite de délivrance. La commande doit être exécutée dans un délai maximum de trente jours à partir du jour de la confirmation de la réception de la commande du cyber acheteur, sauf si les deux parties sont convenus autrement conformément aux dispositions de l'article 39 de la loi 31-08. Lorsque le délai convenu par les deux parties est dépassé de plus de sept jours, le cyber acheteur a le droit de résilier le contrat sans besoin d'une action en justice. Ce droit doit strictement être exercé dans un délai de cinq jours qui suivent l'expiration du délai de sept jours. Il se peut que le contrat électronique mentionne une clause précisant que le délai de délivrance est juste à titre indicatif, et il n'engage pas de responsabilité du cyber commerçant, mais on précise qu'il s'agit d'une clause abusive, qui ne respecte pas les règles législatives en vigueur. De même si le cyber commerçant ne délivre pas la chose objet du contrat pour une

raison d'indisponibilité, il doit en informer le cyber acheteur, qui a le droit d'être remboursé sans délai, et au plus tard dans les quinze jours suivant le paiement du prix qu'il a déjà versé au cyber commerçant. En revanche, si le montant convenu par le contrat électronique est inférieur à 3 000 dirhams, et que le cyber commerçant n'a pas délivré la chose dans le délai imparti, le cyber acheteur est obligé d'intenter une action de résolution.

Cette distinction opérée par le législateur marocain en fonction du montant de la commande ne figure pas en droit français. En effet, dans le cas des contrats électroniques, l'article L. 216-1 du Code de la consommation évoque un délai maximal de 30 jours suivant la confirmation de la commande, sauf en cas de force majeure.

Par conséquent, l'obligation de délivrance de la chose par le cyber commerçant est essentielle dans le contrat électronique, car elle repose sur la confiance de l'acheteur quant à la conformité et la livraison du produit.

ii La garantie de la chose vendue

Le législateur marocain règlemente la garantie de la chose vendue par les articles 549 à 575 du Dahir des obligations et contrats. Le cyber commerçant doit garantir la possession paisible et la jouissance de la chose objet du contrat électronique, ce qui constitue une garantie d'exécution. Ensuite, il est tenu de garantir le cyber commerçant contre les défauts de cette chose, ce qui représente une garantie des vices rédhibitoires.

Dans ce contexte, les dispositions de l'article 571 du Dahir des obligations et contrats prévoit que le cyber commerçant n'est pas tenu de répondre des vices rédhibitoires que dans deux cas d'exception :

- Lorsqu'il les a déjà déclarés au cyber acheteur, en lui informant de tous les vices entachant la chose objet de la vente. C'est une obligation d'information par le cyber commerçant, qui doit être accepté par le cyber acheteur.
- Lorsque le cyber commerçant stipule dans le contrat électronique qu'il n'est tenu d'aucune garantie.

En revanche, il convient de préciser que cette disposition juridique ne s'applique pas aux contrats de vente de produits ou de biens entre le consommateur et le fournisseur, c'est ce qui ressort de l'article 65 de la loi n° 31-08 relative à la protection du consommateur.

Conformément aux dispositions de l'article 65 de la loi 31-08, le délai d'exercice d'une action en justice relative aux défauts de la chose vendue est de deux ans pour les biens immeubles, et une année pour les biens meubles. En France, outre les procédures judiciaires, l'acheteur dispose d'outils spécifiques pour faire valoir ses droits en cas de non-conformité ou de vice

résultant d'une transaction électronique. En effet, il dispose de procédures simplifiées tels que la médiation en ligne qui est un recours effectué auprès des plateformes de règlement des litiges électroniques comme la plateforme ODR de l'Union Européenne.

En général, le cyber commerçant est responsable de cette garantie légale imposée par la loi. En revanche le cyber commerçant peut ajouter des garanties conventionnelles supplémentaires. Dans ce cas, il est tenu de les mentionner dans le contrat électronique, en précisant aussi leur portée, durée, et conditions.

L'obligation de garantir la chose vendue renforce ainsi la confiance dans le contrat électronique en assurant au cyber acheteur que le produit sera conforme et exempt de vices. Cette confiance est essentielle, car elle repose sur la transparence du cyber commerçant, qui doit informer l'acheteur de l'état réel du bien et respecter les garanties légales ou conventionnelles précisées dans le contrat.

Après avoir examiné les obligations du cyber commerçant, qu'en est-il des obligations du cyber acheteur dans le cadre du contrat électronique ?

3.1.2 Les obligations du cyber acheteur

Dans le cadre de l'exécution du contrat électronique, le cyber acheteur est tenu de certaines obligations pour honorer ses engagements et garantir une bonne exécution. Il doit ainsi payer le prix convenu et prendre livraison de la chose. Toutefois, en raison de la relation de confiance qui sous-tend le contrat électronique, il bénéficie également d'un droit de rétractation que nous verrons par la suite.

Cette confiance mutuelle, qui repose sur la transparence des informations et le respect des engagements, est essentielle pour assurer une exécution sereine du contrat. C'est pourquoi il est crucial d'analyser les modalités de paiement (i), et les conditions de réception de la chose dans ce contexte (ii).

i Le paiement du prix convenu

Le cyber acheteur doit payer le prix convenu à la date et de la manière stipulées dans le contrat. À défaut de ces mentions, il est tenu de régler le prix au moment de la délivrance de la chose vendue. Le paiement dans les contrats électroniques peut être effectué de manière physique lors de la livraison ou par voie électronique, cette dernière nécessitant une vigilance particulière de la part du cyber acheteur.

En effet, la confiance dans le contrat électronique repose sur la sécurité des transactions. Le cyber commerçant doit garantir la sécurité des moyens de paiement, en assurant une authentification forte et le respect de la confidentialité des données personnelles. Pour renforcer

cette confiance, le législateur marocain a mis en place la loi 43-20 relative aux services de confiance pour les transactions électroniques. Cette loi vise à sécuriser les contrats électroniques en obligeant les cybers commerçants à obtenir une authentification de leur site via un certificat électronique délivré par un prestataire agréé de services de confiance. Ces mesures sont essentielles pour protéger le cyber acheteur tout au long de la conclusion et de l'exécution du contrat électronique, renforçant ainsi la confiance nécessaire dans ces transactions.

Quant à la loi française, l'article L. 221-5 du Code de la consommation impose des obligations supplémentaires au vendeur afin de protéger le consommateur et maintenir la confiance dans le contrat électronique. De plus, l'article L. 112-12 du Code monétaire et financier interdit les surcoûts pour l'utilisation de certains moyens de paiement. Comme au Maroc, le vendeur doit également indiquer les modalités de paiement acceptées et préciser, le cas échéant, les échéances ou conditions de financement. En l'absence de ces informations, le contrat peut être annulé ou déclaré nul. La confiance, essentielle dans les contrats électroniques, se renforce en France par la directive européenne DSP2, qui impose une authentification forte pour les paiements électroniques, garantissant ainsi la sécurité de la transaction. En cas de fraude résultant d'un manquement à ces obligations, l'acheteur est en droit d'engager la responsabilité du vendeur. Enfin, le vendeur est tenu d'utiliser des outils sécurisés pour protéger les données de paiement, conformément à l'article L. 133-16 du Code monétaire et financier et au RGPD, renforçant ainsi la confiance dans l'environnement numérique.

Par ailleurs, lorsque le cyber acheteur choisit le paiement électronique, qui consiste à transférer une somme d'argent par voie électronique, il doit respecter les délais de paiement et, surtout, vérifier la sécurité du site de paiement proposé par le cyber commerçant. La confiance dans le contrat électronique repose ici sur la transparence et la sécurité des transactions.

Dans cette optique, le cyber acheteur doit procéder au paiement selon la modalité convenue (par virement, carte bancaire, mobile « M-wallet », etc.), en conformité avec les clauses contractuelles et les lois en vigueur. Pour garantir l'interopérabilité des paiements électroniques par carte bancaire, les établissements de crédit ont créé en 2001 le Centre Monétique Interbancaire (CMI), chargé de centraliser le traitement des opérations monétiques au niveau national. En ce qui concerne les paiements électroniques internationaux, la loi type de la CNUDCI sur les virements électroniques offre un cadre orienté vers la régulation de ces transactions. La confiance dans ce cadre repose sur le respect des règles de sécurité et des obligations légales.

La responsabilité du cyber acheteur est engagée en cas de défaut de paiement dans les délais convenus, mais celle du cyber commerçant l'est également s'il néglige de mettre en place un système de sécurité adéquat. Il doit se conformer aux exigences de la loi 43-20, qui régit les moyens de cryptologie pour assurer la protection des transactions.

Après le paiement, le cyber acheteur est tenu de prendre livraison de la chose, renforçant ainsi la confiance dans l'exécution du contrat électronique.

ii La prise de livraison de la chose objet du contrat

Dans le cadre des contrats électroniques, la confiance entre le cyber acheteur et le cyber commerçant repose sur l'exécution fidèle des engagements, y compris la prise de livraison de la chose objet du contrat à la date et au lieu convenus. Le cyber acheteur doit retirer le produit ou service à l'endroit spécifié, qu'il s'agisse de son domicile ou d'un autre lieu déterminé d'un commun accord.

Dans la pratique du commerce électronique, la plupart des livraisons des biens vendus sont effectuées au domicile du cyber acheteur ou à l'adresse convenue entre les parties. Si le cyber acheteur ne prend pas livraison de la marchandise, sa responsabilité est engagée. Dans ce cas, les règles générales de mise en demeure s'appliquent, conformément au premier alinéa de l'article 580 du Dahir des obligations et contrats. Si aucune action n'est entreprise après la mise en demeure, le contrat peut être résolu. En droit français, le vendeur peut également adresser une mise en demeure au consommateur. Si cette mise en demeure reste sans effet, le vendeur peut envisager la résolution du contrat et demander des dommages et intérêts pour couvrir les frais de stockage et de réexpédition. Ces principes de mise en demeure et de résolution du contrat sont similaires tant en droit marocain qu'en droit français.

Dans le cas de défaut de paiement, le cyber commerçant peut arrêter la vente ou revendiquer la chose vendue si elle a été prise par l'acheteur sans règlement. La revendication doit intervenir dans un délai de 15 jours après la remise de la chose. Si le contrat prévoit une clause de résolution en cas de non-paiement, celui-ci est résolu automatiquement en l'absence de règlement dans les délais fixés. Ce cadre juridique repose sur une relation de confiance : l'acheteur est censé respecter ses engagements, et le vendeur doit garantir un processus de transaction sécurisé et transparent. Ce principe de confiance est crucial, notamment en ce qui concerne l'exécution des contrats électroniques, qui soulève des enjeux importants en matière de protection des consommateurs et de cybersécurité.

3.2 Les enjeux de l'exécution des contrats électroniques

L'exécution des contrats électroniques soulève plusieurs enjeux, notamment en matière de protection des consommateurs et de sécurité des transactions. Dans ce chapitre, nous aborderons d'abord les problématiques liées à la protection du cyberconsommateur, en mettant en lumière les mécanismes juridiques et les pratiques visant à garantir ses droits (3.2.1). Ensuite, nous explorerons les enjeux de la cybersécurité, essentiels pour assurer des échanges numériques fiables et sécurisés (3.2.2). Ces deux aspects sont cruciaux pour garantir la confiance et la fiabilité des contrats électroniques.

3.2.1 La sécurisation de la confiance des cyberconsommateurs dans les contrats électroniques

L'essor de l'e-commerce a transformé les pratiques de consommation au Maroc, mettant en lumière des enjeux cruciaux en matière de protection des cyberconsommateurs. Face à l'expansion rapide des transactions en ligne, il devient essentiel de garantir un cadre juridique adapté pour sécuriser les droits des consommateurs tout en préservant la confiance dans le système juridique. Toutefois, cette protection juridique se heurte à des défis majeurs, notamment la mise en œuvre effective des textes législatifs et les pratiques commerciales parfois défaillantes. Dans cette section, nous examinerons d'une part les dispositifs juridiques mis en place pour protéger le consommateur électronique (i) et, d'autre part, les réalités pratiques de cette protection (ii), en soulignant les avancées réalisées et les difficultés persistantes.

i Les dispositifs juridiques de la protection du cyberconsommateur

L'adoption de la loi n° 31-08, entrée en vigueur en avril 2011, constitue une étape majeure dans le développement de la protection du consommateur électronique au Maroc. Ce texte législatif vise à instaurer des règles strictes pour encadrer les transactions en ligne, afin de garantir une meilleure sécurité juridique pour les cyberconsommateurs. La loi impose aux fournisseurs de biens et services en ligne une série d'obligations de transparence et d'information préalable, qui sont essentielles pour assurer une consommation éclairée. Ainsi, les consommateurs doivent être informés de manière claire et exhaustive sur les caractéristiques essentielles des produits ou services, leur prix, les conditions de garantie, les modalités de livraison, ainsi que sur toute autre information pertinente avant la conclusion du contrat. Cette exigence permet de réduire le risque de litiges en offrant aux consommateurs les informations nécessaires pour faire un choix éclairé. En outre, la loi garantit un droit fondamental : celui de rétractation. Ce droit permet au consommateur de se retirer du contrat dans un délai de 7 jours après l'achat, période

qui peut être prolongée à 30 jours si l'information n'a pas été fournie de manière conforme. En droit français, ce délai est fixé à 14 jours, conformément à l'article L. 221-18 du Code de la consommation. Ce droit constitue une avancée importante, puisqu'il offre une protection supplémentaire face à des achats réalisés à distance, où l'absence de contact direct avec le produit peut induire un sentiment d'incertitude chez le consommateur.

Cependant, la loi n° 31-08 ne s'arrête pas à la protection de l'information préalable ; elle introduit également des garanties contre certaines pratiques commerciales abusives, telles que la vente forcée, ou l'usage de clauses abusives dans les contrats électroniques. Les fournisseurs sont également tenus de respecter une délivrance d'un document écrit ou d'un support durable confirmant les termes du contrat, ce qui vise à renforcer la sécurité juridique des consommateurs et à éviter toute ambiguïté.

Dans une optique d'amélioration continue de la protection des cyberconsommateurs, la loi n° 78-20, promulguée en décembre 2020, a marqué une avancée significative en matière de réglementation des contrats électroniques. Cette loi a apporté des clarifications essentielles, notamment en ce qui concerne la compétence judiciaire en cas de litige entre un consommateur et un fournisseur. Avant cette loi, l'application de la loi n° 31-08 créait des zones d'incertitude sur la juridiction compétente, certains tribunaux commerciaux étant appelés à trancher des différends où les consommateurs se retrouvaient souvent dans une position désavantageuse. La loi n° 78-20 a permis de rétablir un équilibre en attribuant explicitement la compétence aux tribunaux de première instance, souvent plus proches des consommateurs, et donc plus accessibles. En France, cette compétence appartient au Tribunal judiciaire lorsque le consommateur est un particulier, et au Tribunal de commerce si le consommateur agit en qualité de professionnel.

Ce renforcement législatif contribue à la création d'un environnement de confiance, où les relations commerciales en ligne sont encadrées de manière plus rigoureuse, permettant ainsi de sécuriser les transactions et de protéger les droits des consommateurs face aux risques de fraude, d'abus ou d'omission d'information. Toutefois, bien que ce cadre législatif soit désormais plus complet, sa mise en œuvre reste un défi majeur. La protection effective des cyberconsommateurs dépend en grande partie de la vigilance et de l'engagement des autorités publiques, mais aussi de la conformité des acteurs économiques aux normes établies. En effet, malgré l'existence d'un cadre législatif solide, des lacunes dans l'application des règles peuvent encore subsister, ce qui impose une surveillance continue et une mise à jour régulière de la réglementation pour répondre aux nouveaux défis technologiques et commerciaux du marché

numérique.

ii La mise en œuvre de la protection des cyberconsommateurs entre théorie et pratique

La mise en œuvre des lois de protection des cyberconsommateurs a conduit à la création de plusieurs dispositifs de contrôle et de soutien. Le lancement du portail www.khidmat-almostahlik.ma par le ministère de la Réforme de l'Administration et de la Fonction publique est l'une des initiatives clés. Ce site offre aux consommateurs des informations sur leurs droits, permet de déposer des réclamations et facilite l'accès à la législation en vigueur. Il joue un rôle essentiel dans l'information et la sensibilisation des consommateurs aux pratiques commerciales responsables, tout en offrant un canal direct pour faire valoir leurs droits.

Les associations de protection des consommateurs, telles que celles soutenues par la loi n°31-08, ont également contribué à la défense des droits des cyberconsommateurs. Par exemple, ces associations offrent des conseils gratuits et assistent les consommateurs dans la résolution amiable des litiges. Le rôle de ces associations est primordial, notamment dans le cadre de la médiation entre consommateurs et fournisseurs, où les résultats sont souvent positifs.

En outre, des efforts notables ont été réalisés pour renforcer la conformité des sites de commerce électronique à la loi. La Cellule de contrôle des sites marchands, ainsi que la Commission Nationale de Protection des Données Personnelles (CNDP), ont mené plusieurs actions de contrôle qui ont permis de détecter des infractions et de sanctionner les sites non conformes aux règles de protection des données personnelles.

Malgré ces réalisations, des défis persistent dans la mise en œuvre effective de la protection des cyberconsommateurs. Une des difficultés majeures réside dans la méconnaissance des droits par les consommateurs eux-mêmes. Beaucoup de cyberconsommateurs ne sont pas pleinement informés de leurs droits, ce qui limite leur capacité à revendiquer une protection adéquate en cas de litige. Le manque de sensibilisation et de formation dans ce domaine, en particulier dans les zones rurales, reste un obstacle important.

De plus, bien que la loi 31-08 offre des garanties, certaines pratiques abusives persistent dans le domaine de l'e-commerce. De nombreux sites marchands ne respectent pas toujours les exigences légales, en particulier en ce qui concerne la transparence des informations ou le respect des délais de livraison. Les clauses abusives, comme celles qui favorisent un déséquilibre contractuel en faveur des fournisseurs, sont encore présentes dans certains contrats électroniques, ce qui rend la situation moins favorable pour les consommateurs.

Les associations de consommateurs, bien qu'actives, manquent de moyens pour mener des actions judiciaires en cas de violation des droits des cyberconsommateurs. La possibilité de

porter plainte collectivement n'est pas toujours clairement définie, et les associations n'ont pas toujours les ressources nécessaires pour organiser des actions en justice. Ce manque de moyens peut nuire à l'efficacité du système de protection.

Enfin, certains acteurs du marché ignorent encore les obligations imposées par la loi, notamment en matière de sécurité des données et de respect des droits à l'information. Des réformes supplémentaires sont donc nécessaires pour garantir que les structures administratives et les associations de consommateurs soient mieux équipées pour défendre les droits des citoyens à l'ère du numérique.

Dans cette optique, il est crucial de considérer la cybersécurité non seulement comme un enjeu technique, mais aussi comme un outil fondamental pour assurer la protection des contrats électroniques, en renforçant ainsi la confiance des utilisateurs dans les échanges numériques.

3.2.2 La cybersécurité au service de la protection des contrats électroniques

La cybersécurité est un enjeu majeur pour garantir la validité et la sécurité des transactions numériques dans le cadre des contrats électroniques. En effet, la confiance des parties prenantes dans l'intégrité, la confidentialité et la disponibilité des informations échangées est essentielle pour le bon déroulement de ces contrats. Toutefois, cette confiance juridique repose non seulement sur des mécanismes techniques de sécurisation, mais également sur un cadre législatif et institutionnel robuste, qui permet de répondre aux défis posés par la cybercriminalité et les risques technologiques. Dans cette section, nous examinerons les principaux défis liés à la cybersécurité dans le domaine des contrats électroniques (i). Nous aborderons également le rôle crucial joué par la cybersécurité pour assurer la confiance dans les transactions numériques et renforcer la fiabilité des systèmes d'information (ii).

i Les défis d'implémentation de la cybersécurité

Le Maroc a progressivement mis en place un cadre juridique et réglementaire pour encadrer la cybersécurité, notamment à travers la loi 09-08 de 2009 relative à la protection des données personnelles, la loi 53-05 sur les échanges électroniques, et la Directive nationale de la sécurité des systèmes d'information (DNSSI). Ces législations ont pour objectif de renforcer la confiance dans les transactions électroniques en protégeant les données personnelles et en garantissant la sécurité des systèmes d'information.

Cependant, la mise en œuvre de ces réformes rencontre plusieurs obstacles. D'une part, bien que les lois soient modernes, leur adoption par certains acteurs judiciaires est lente, et certains magistrats restent réticents à les appliquer efficacement, notamment face à la cybercriminalité. Cette situation fragilise la confiance des utilisateurs et des entreprises dans le système juridique,

car la protection des contrats électroniques reste vulnérable face aux défis numériques. En effet, de nombreux juges continuent de se référer aux règles du droit commun pour traiter les affaires de cybercriminalité, ce qui ralentit la réponse judiciaire face aux nouvelles menaces technologiques.

D'autre part, l'adoption inégale des normes de cybersécurité par les entreprises marocaines demeure un défi majeur. Bien que la majorité des entreprises respectent les lois telles que la loi 09-08 et la DNSSI, de nombreuses entreprises ne vérifient pas régulièrement leur conformité, ce qui expose leurs systèmes à des vulnérabilités. Cette lacune dans la sécurité des systèmes d'information fragilise la confiance des utilisateurs dans la validité et la sécurité des contrats électroniques.

Enfin, le manque de formation continue sur la cybersécurité, tant pour les acteurs publics que privés, complique encore la mise en œuvre efficace de ces réformes. Pour que les entreprises puissent garantir la sécurité de leurs systèmes d'information et, par conséquent, la validité des contrats électroniques, il est crucial que les régulateurs et les juges soient également formés aux défis technologiques actuels.

Dans ce contexte, des initiatives comme la coopération avec des organismes internationaux tels que l'Union internationale des télécommunications (UIT) et la participation du Maroc à des projets régionaux comme CyberSud sont essentielles pour renforcer l'infrastructure juridique et technique en matière de cybersécurité. Cela contribuerait à restaurer la confiance des citoyens et des entreprises dans les transactions électroniques et à sécuriser les relations contractuelles dans l'environnement numérique.

ii Les atouts de la cybersécurité en faveur des contrats électroniques

La cybersécurité est un pilier central pour établir la confiance dans le cadre des contrats électroniques. En effet, dans un environnement numérique où les parties à un contrat échangent des informations sensibles à distance, la sécurisation des transactions devient indispensable pour garantir leur validité et leur efficacité. L'élément fondamental réside dans la protection des données personnelles et des informations confidentielles, essentielles pour que les acteurs impliqués dans le contrat aient confiance dans l'intégrité des informations échangées.

La cybersécurité permet de garantir plusieurs principes cruciaux pour la conclusion et l'exécution d'un contrat électronique : la disponibilité des systèmes, l'intégrité des données, la confidentialité des informations, et la non-répudiation des actions. Ces principes assurent que les parties peuvent échanger des informations avec la certitude que les données ne seront ni falsifiées ni altérées, et que les transactions seront irrévocables et vérifiables. Sans ces garanties,

la légitimité des contrats électroniques pourrait être remise en question, mettant ainsi en péril l'ensemble du système juridique numérique.

Cette question prend encore plus d'importance dans le contexte de la digitalisation accrue avec l'avènement de l'industrie 4.0, où les systèmes d'information sont de plus en plus intégrés aux infrastructures physiques. Dans ce cadre, la cybersécurité ne concerne plus seulement la protection des données, mais aussi celle des infrastructures critiques, renforçant la sécurité des transactions électroniques au niveau global.

Ainsi, pour que la confiance juridique dans les contrats électroniques soit consolidée, il est crucial que le Maroc continue à renforcer son cadre législatif et institutionnel. Cela inclut non seulement l'amélioration de la législation existante, mais aussi la mise en place de mécanismes de contrôle rigoureux et l'adoption de nouvelles normes de sécurité adaptées aux défis de l'ère numérique. Le rôle de l'État est central, en soutenant une coopération active entre le secteur public et privé, et en encourageant l'évolution des pratiques de cybersécurité à tous les niveaux.

Conclusion

La confiance est le pilier essentiel de la contractualisation électronique, tant dans sa formation que dans son exécution. Ce processus repose sur une dualité : le respect des principes juridiques classiques et l'intégration de mécanismes technologiques adaptés aux spécificités du numérique.

Dans un premier temps, l'article a démontré que les fondements de la confiance dans la formation du contrat électronique s'articulent autour de la validité juridique et des mécanismes d'authentification. Si le contrat électronique offre des opportunités d'agilité et d'accessibilité, il n'échappe pas aux contraintes du formalisme juridique traditionnel. Les obstacles liés à la sécurité des échanges, à l'identification des parties et à la validité des consentements ont été mis en lumière. En réponse, la e-signature et la certification des prestataires de services apparaissent comme des solutions fiables, encadrées par des dispositifs normatifs renforçant l'authenticité et la sécurité des transactions numériques.

Ensuite, la seconde partie de l'article a souligné les enjeux de la confiance dans l'exécution des contrats électroniques, notamment à travers les obligations respectives des parties. Le cyber commerçant doit garantir la transparence et la sécurité des transactions, tandis que le cyber acheteur doit agir de manière diligente et sécurisée. En outre, l'instauration de la confiance juridique nécessite une protection accrue des cyberconsommateurs et une cybersécurité adaptée aux menaces actuelles. La sécurisation des données personnelles et la prévention des attaques numériques se positionnent désormais comme des conditions sine qua non pour garantir la pérennité et la légitimité des contrats électroniques.

En conclusion, pour que la confiance dans le contrat électronique soit durable, il est nécessaire d'assurer un équilibre entre l'évolution technologique et la régulation juridique. Le renforcement de la cybersécurité et l'adaptation continue des dispositifs normatifs contribueront à préserver cette confiance indispensable. À terme, cela pourrait également inciter le législateur à approfondir les cadres existants, en anticipant les enjeux futurs liés à l'émergence de nouvelles technologies comme l'intelligence artificielle et la blockchain.

REFERENCES

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). (2023). "Normes et protocoles pour la cybersécurité au Maroc". ANSSI. https://www.anssi.ma.

BENOTMANE, R. (2016). Le régime juridique de la vente à distance en droit marocain, éditions universitaires européennes.

BENSOUSSAN, A. (2017). Informatique et Télécom, 1ère éd., Francis Lefère.

Blanchot, F, La confiance à l'ère du numérique. (2020/4). in Doueihi, M. & Domenicucci, J. (dir.), RIMHE : Revue Interdisciplinaire Management, Homme & Entreprise, n° 41, vol. 9, Paris, Berger Levrault/Rue d'Ulm, Coll. Au fil du débat.

BOUKBIR, A., « La preuve électronique des transactions commerciales au Maroc à la lumière de la loi 53-05 », Revue des sciences juridiques, disponible sur : https://www.marocdroit.com/.

BRUGUIERE, J.-M., « L'exécution du contrat électronique », dans Le contrat électronique au cœur du commerce électronique, le droit de la distribution : Droit commun ou droit spécial ?, Journées d'études du 10 mars 2005 et 15 mars 2004 organisées par le DJCE de Poitiers, Coll. de la Faculté de droit et des Sciences sociales, 2005.

CNUDCI, Loi type de la CNUDCI sur les virements internationaux. (1992). Commission des Nations Unies pour le Droit Commercial International.

CNUDCI, Loi-type sur le commerce électronique. (1996). Commission des Nations Unies pour le Droit Commercial International.

Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP). (2023). "Le RGPD et son impact au Maroc". CNDP. https://www.cndp.ma.

Convention des Nations Unies sur l'utilisation des communications électroniques dans les contrats internationaux. (2005).

COSTES, L. (février 2000). Transactions en ligne, preuve et signature, Lamy, Droit de l'informatique et des réseaux, N°122.

Dahir des Obligations et des Contrats (DOC), articles 417-1, 417-2, et 417-24, modifiés par la loi n° 53-05.

DATAPROTECT/AUSIM. (Juin 2018). Les enjeux de la cybersécurité au Maroc, Livre Blanc, Bibliothèque Nationale du Royaume du Maroc.

Denis, A. (2021). La confiance dans les transactions électroniques : Enjeux technologiques et légaux. Presses Universitaires de France.

Directive 2000/31/CE, sur le commerce électronique dans le marché intérieur européen.

EDDEROUASSI, M. (2017). Le contrat électronique international, Thèse pour l'obtention du

doctorat en droit privé, Université Grenoble APLS.

GHOLI, M. & FASLY, H. (2019). « La sécurité des échanges électroniques : cas de gouvernement électronique », Revue internationale des sciences de gestion, N°6 / Volume 3, N°1, pp. 869-889.

JACQUEMIN, H. (2012). « Contrats en ligne et protection du consommateur numérique », J.T., n° 40.

KEMPF, O., MAZZUCCHI, N. (2015/5). « Cyberespace et intelligence économique », Géoéconomie, (N° 77).

LE CROSNIER, H., « Internet et numérique ». (2011). dans D. Ventre, Cyberespace et acteurs du cyberconflit, Collection Cyberconflits et cybercriminalité, Ed. Lavoisier.

LEROYER, A. (2002). L'épreuve d'Internet, faut-il recodifier le droit de la consommation ?, Economica.

Loi n° 05-20 relative à la cybersécurité

Loi n° 24-96 relative à la poste et aux télécommunications

Loi n° 31-08 relative à la protection du consommateur, Maroc.

Loi n° 43-20 relative aux services de certification électronique, Maroc.

Loi n° 53-05 relative à l'échange électronique de données juridiques, Maroc.

MARCUS, L. (9 décembre 2015). « La sécurisation des transactions électroniques : vers un marché numérique européen », www.ceje.ch.

MUR S. (2021). « Le point sur le règlement eIDAS, cadre européen pour la signature électronique », Appvizer.

Note d'information de Bank Al Maghrib, Numéro 4 (janvier 2010), Systèmes et moyens de paiement au Maroc : rôle et responsabilités de Bank Al-Maghrib, sur : https://www.bkam.ma/content/download/.

OLY, C.-R. (2005). Le paiement en ligne : sécurisation juridique et technique, Paris, Hermes Science.

Règlement eIDAS (UE) n° 910/2014, sur l'identification électronique et les services de confiance.

STONFEL MUNCK, P. (2004). « La réforme des contrats du commerce électronique », JCP E, I.

VENTRE, D. (2011). « Cyberespace et acteurs du cyberconflit », Cyberconflits et cybercriminalité, Ed. Lavoisier.

Von Solms, Rossouw, et Van Niekerk, Johan, From information security to cyber security,

Computers and Security, vol. 38, p. 97-102, https://doi.org/10.1016/j.cose.2013.04.004.

Yammahi, S. (2008). La protection du consommateur dans les contrats électroniques de consommation (Thèse de doctorat, Université de Rouen). Version validée par le jury, dépôt national, reproduction conforme.