Revue Internationale du Chercheur
ISSN: 2726-5889
Volume 6 : Numéro 4

La digitalisation des transactions commerciales au Maroc : apports, limites et enjeux de la sécurité juridique

The digitization of commercial transactions in Morocco: benefits, limitations, and legal certainty issues.

Yahaya Hamidou Abdoul Jalili

Doctorant en droit privé

Laboratoire des Sciences Juridiques et Sociales

Université Mohamed Premier – Oujda

Maroc

Date de soumission : 27/10/2025

Date d'acceptation : 10/12/2025

Pour citer cet article :

Yahaya Hamidou A. J. (2025) «La digitalisation des transactions commerciales au Maroc : apports, limites et enjeux de la sécurité juridique », Revue Internationale du chercheur « Volume 6 : Numéro 4 » pp : 1559-1577

Résumé
La digitalisation des transactions commerciales s'impose aujourd'hui comme un levier majeur de modernisation de l'économie marocaine. Accélérée par les réformes juridiques (notamment la loi 53-05 relative à l'échange électronique de données juridiques et la loi 09-08 sur la protection des données personnelles ainsi que la loi n°43-20 relative aux services de confiance pour les transactions électroniques) cette transformation introduit des outils innovants tels que les plateformes numériques, la signature électronique, la blockchain, les ERP et les paiements électroniques.
Toutefois, l'essor rapide de ces mécanismes soulève d'importants enjeux de sécurité juridique touchant la force probante des documents électroniques, la responsabilité des prestataires techniques, la cybersécurité, les risques de fraude numérique et la protection des données.
S'appuyant sur une méthodologie qualitative fondée sur l'analyse doctrinale, normative et institutionnelle, cet article examine de manière approfondie le cadre juridique encadrant les transactions numériques, les bénéfices opérationnels de la digitalisation et les limites structurelles auxquelles restent confrontés les opérateurs économiques. Il propose également une synthèse des travaux antérieurs issus de la Revue CCA, de la Revue Belge et de la Revue Francophone des Études Multidisciplinaires, permettant de situer la présente étude dans une perspective scientifique consolidée. Les résultats montrent que la sécurité juridique, condition essentielle de la confiance numérique, nécessite une harmonisation normative, un renforcement institutionnel et une modernisation des outils de régulation.
Mots-clés : Digitalisation, Transactions commerciales, Sécurité juridique, Signature électronique, Protection des données personnelles.

Abstract
Digitalization has become a key driver of Morocco's economic modernization, notably through legal reforms such as Law 53-05 on electronic data exchange and Law 09-08 on personal data protection. This technological transformation has fostered the adoption of digital tools including electronic platforms, electronic signatures, blockchain systems, ERP solutions and electronic payment mechanisms. However, this rapid shift raises fundamental legal security issues related to the evidentiary value of electronic documents, the liability of technical service providers, cybersecurity threats, digital fraud risks and data protection obligations.
Based on a qualitative methodology combining doctrinal, normative and institutional analysis, this article provides an in-depth assessment of the legal framework governing digital commercial transactions in Morocco. It examines the operational benefits of digitalization, identifies the persistent structural challenges, and offers a critical reading of previous research published in CCA, the Belgian Review, and the Francophone Review of Multidisciplinary Studies. Findings show that legal security remains a central pillar for strengthening trust in the digital environment, and that Morocco must reinforce its regulatory framework, modernize its institutional mechanisms and align with international best practices to ensure secure and reliable digital transactions.
Keywords : Digitalization, Commercial transactions, Legal security, Electronic signature, Data protection.

Introduction

De prime abord, la digitalisation constitue aujourd'hui un axe stratégique de transformation de l'économie marocaine. L'essor du commerce électronique, la dématérialisation des services publics, l'utilisation accrue des plateformes numériques et l'essor des paiements digitales témoignent d'une mutation profonde des modes de contractualisation, de gestion et de règlement des transactions. Le Maroc, en suivant les recommandations de l'OCDE, de l'UNCTAD et de la CNUDCI, a engagé un ensemble de réformes visant à renforcer la confiance des acteurs économiques et à sécuriser les échanges en ligne.

Toutefois, cette évolution n'est pas dénuée d'enjeux. La digitalisation crée de nouvelles vulnérabilités liées à la cybersécurité, à la responsabilité des prestataires techniques, aux violations de données personnelles, à l'usurpation d'identité et à la fiabilité de la preuve numérique. La sécurité juridique, entendue comme la prévisibilité de la norme, la stabilité des règles et l'efficacité des mécanismes de protection, s'impose ainsi comme une condition essentielle de l'essor du commerce électronique. Comme le soulignent Adler (2002) et Schuller et al. (2000), la confiance constitue l'élément fondateur de toute relation commerciale, particulièrement en environnement numérique.

Cette étude est guidée par trois interrogations centrales : le cadre juridique marocain assure-t-il une protection suffisante des transactions numériques ? Les dispositifs techniques, tels que les plateformes, les systèmes de paiement et les signatures électroniques, garantissent-ils une sécurité juridique satisfaisante ? Quelles réformes sont nécessaires pour renforcer la confiance numérique et sécuriser durablement les échanges ?

Les objectifs de la recherche sont d'analyser le cadre normatif marocain régissant les transactions électroniques, d'évaluer les bénéfices et les limites opérationnelles de la digitalisation, d'examiner les défis juridiques persistants, et de formuler des recommandations visant à renforcer la sécurité juridique des échanges numériques.

Cette recherche adopte une démarche qualitative combinant l'analyse doctrinale et juridique des lois marocaines, de la jurisprudence et des normes internationales, l'examen de rapports institutionnels de la CNDP, de Bank Al-Maghrib et du ministère du Commerce, ainsi qu'une approche comparative avec l'Union européenne, le règlement eIDAS et l'UNCITRAL. Elle s'appuie enfin sur une synthèse critique de travaux scientifiques, afin d'éclairer les apports, les

limites et les enjeux de la sécurité juridique liés à la digitalisation des transactions commerciales au Maroc.

1. La digitalisation des transactions commerciales au Maroc : cadre juridique, outils et pratiques

1.1. Le cadre juridique encadrant les transactions numériques

1.1.1. La signature électronique : validité, force probante et responsabilités

La signature électronique, consacrée par la loi 53-05, constitue le fondement juridique de la contractualisation numérique. Elle repose sur des mécanismes cryptographiques permettant d'assurer l'identification du signataire et l'intégrité du document.

Cette loi établit l'« équivalence fonctionnelle » entre le support électronique et le support papier, principe largement inspiré des règles d'UNCITRAL et des standards européens eIDAS.

La distinction entre signature simple, avancée et sécurisée (cette dernière reposant sur un dispositif de création de signature qualifié et un certificat électronique) revêt une importance capitale en matière probatoire. Plus le dispositif est sécurisé, plus la signature bénéficie d'une présomption de fiabilité.

Toutefois, la doctrine marocaine (Benkirane, 2020 ; Tahiri, 2021) souligne que les tribunaux sont encore peu confrontés à ces instruments, ce qui crée une incertitude sur la manière dont la preuve électronique sera appréciée en cas de litige.
La responsabilité des prestataires de certification, essentiels dans ce mécanisme, demeure un point sensible : absence de réglementation détaillée, opacité des obligations contractuelles, difficulté à déterminer les responsabilités en cas de défaillance technique. Cela constitue un obstacle à la confiance dans l'environnement numérique.

1.1.2. La protection des données personnelles et les obligations des acteurs

A l'instar de la loi n°43-20 relative aux services de confiance pour les transactions électroniques, la loi 09-08 constitue l'un des piliers de la sécurité juridique des transactions numériques. Elle encadre la collecte, le traitement, la conservation et la protection des données personnelles. Les entreprises doivent respecter les principes de finalité, de proportionnalité, de légitimité et de sécurité, sous le contrôle de la CNDP.

Les rapports annuels de la CNDP révèlent que de nombreuses entreprises, notamment des PME, ne respectent pas leurs obligations déclaratives ou n'adoptent pas des mesures de cybersécurité adéquates. Les risques de violation de données, de piratage ou d'usurpation d'identité augmentent en conséquence. Comparé au RGPD européen, le cadre marocain reste moins exigeant : absence de notification obligatoire des violations, sanctions limitées, faible culture de conformité.
Dans un environnement commercial digitalisé, cette faiblesse constitue un obstacle important à la confiance des utilisateurs et des partenaires internationaux.

1.1.3. Les normes sectorielles et internationales

Au-delà des lois générales encadrant la transformation numérique, un ensemble de textes sectoriels vient compléter le cadre juridique marocain.

La réglementation des télécommunications définit les obligations des opérateurs et assure la protection des utilisateurs dans un contexte de convergence numérique.

Les règles édictées par Bank Al-Maghrib encadrent les services de paiement et garantissent la sécurité des transactions électroniques.

De même, la législation relative aux marchés publics électroniques fixe les conditions de dématérialisation des procédures publiques, tandis que les directives de l'ANRT sur la certification électronique contribuent à renforcer la fiabilité et la validité juridique des signatures numériques.

Parallèlement, les normes et standards internationaux jouent un rôle déterminant dans l'orientation et l'harmonisation des pratiques numériques.

Le règlement eIDAS de l'Union européenne, relatif à l'identification électronique et aux services de confiance, sert de référence pour la mise en place de systèmes sécurisés et reconnus. Les modèles de contrats et recommandations de la Commission des Nations Unies pour le droit commercial international (UNCITRAL) fournissent des lignes directrices pour la conclusion de transactions électroniques transfrontalières.

Les normes ISO, notamment la série ISO 27000 sur la cybersécurité, fixent des standards de sécurité et de gestion des risques essentiels pour protéger les systèmes d'information et les données sensibles.

Cependant, cette pluralité de normes, nationales et internationales, entraîne une certaine fragmentation du cadre juridique.

La coexistence de textes divers peut rendre difficile la lisibilité et l'application cohérente des règles pour les entreprises et les administrations. Elle nécessite un effort constant d'harmonisation et de coordination afin d'assurer une sécurité juridique optimale et de faciliter l'adoption des technologies numériques dans un environnement légal clair et stable.

1.2. Les plateformes et infrastructures numériques

1.2.1. Plateformes publiques : dématérialisation et transparence

Le portail national des marchés publics représente un exemple probant de réussite dans la digitalisation des procédures administratives. Cette plateforme centralisée permet d'assurer une traçabilité complète des transactions et des décisions, tout en garantissant l'intégrité et la transparence des processus d'attribution des marchés.

Les soumissionnaires bénéficient ainsi d'un accès équitable à l'information, réduisant les asymétries et favorisant une concurrence loyale. En outre, la dématérialisation contribue à raccourcir significativement les délais de traitement des dossiers et à limiter les risques de pratiques corruptives, offrant un environnement plus fiable pour les acteurs économiques.

Cependant, malgré ces avancées, certaines contraintes demeurent.

D'une part, des difficultés techniques, telles que des problèmes d'accessibilité ou de performance de la plateforme, peuvent entraver l'expérience utilisateur.

D'autre part, l'accompagnement des petites et moyennes entreprises reste insuffisant, limitant leur capacité à tirer pleinement parti de ces outils numériques.

Enfin, l'interopérabilité entre le portail et les systèmes internes des différentes administrations est encore partielle, ce qui peut générer des redondances, ralentir le traitement des données et limiter l'efficacité globale du dispositif.

Ainsi, si la plateforme constitue une avancée majeure vers une administration plus transparente et efficiente, un renforcement de l'assistance aux utilisateurs et une meilleure intégration des systèmes restent nécessaires pour exploiter tout le potentiel de la dématérialisation.

1.2.2. Plateformes privées : fintechs, ERP, paiement électronique

Les fintechs marocaines connaissent un essor remarquable depuis 2020, porté par le développement rapide des paiements mobiles, des portefeuilles électroniques et des solutions de e-paiement.

Ces innovations facilitent l'inclusion financière, offrent des services plus accessibles aux particuliers et aux petites entreprises, et participent activement à la modernisation du paysage économique.

Selon les données de Bank Al-Maghrib, les transactions électroniques ont enregistré une croissance annuelle moyenne de plus de 20 % entre 2018 et 2023, illustrant l'ampleur de cette transition vers le numérique et l'adoption progressive des outils technologiques par le grand public.

Parallèlement, les systèmes ERP (Enterprise Resource Planning) jouent un rôle central dans l'automatisation des processus internes des entreprises. Ils permettent de gérer efficacement les commandes, la facturation, la comptabilité et le suivi des stocks, tout en renforçant la conformité réglementaire et la traçabilité des opérations. Ces outils offrent une meilleure visibilité sur la gestion financière et opérationnelle, et favorisent une prise de décision plus rapide et éclairée.

Cependant, la dépendance croissante à ces systèmes numériques expose les entreprises à des risques juridiques et opérationnels significatifs. En cas d'erreur algorithmique, de cyberintrusion ou de défaillance technique, les conséquences peuvent être lourdes, notamment sur le plan contractuel et financier.

La législation marocaine demeure encore lacunaire en matière de responsabilité des prestataires de services numériques, laissant des zones d'incertitude sur la répartition des obligations et des recours possibles. Cette situation souligne la nécessité d'un encadrement juridique plus précis pour sécuriser les transactions électroniques et renforcer la confiance des acteurs économiques dans ces outils numériques.

Ainsi, les plateformes privées représentent un moteur puissant de modernisation et d'efficacité pour les entreprises marocaines, mais leur adoption doit s'accompagner de dispositifs de sécurité, de formation et de cadre légal adapté pour en maximiser les bénéfices tout en minimisant les risques.

1.2.3. Blockchain et nouveaux outils de traçabilité

La technologie blockchain se distingue par sa capacité à garantir l'immutabilité des enregistrements et une transparence quasi inatteignable avec les systèmes traditionnels.

Chaque transaction ou opération enregistrée sur la chaîne est horodatée, sécurisée et vérifiable par l'ensemble des participants, ce qui renforce la confiance dans les échanges et la fiabilité des données.

Dans le contexte marocain, cette technologie pourrait offrir des solutions innovantes pour des secteurs variés tels que la logistique, l'agroalimentaire, les transactions financières ou transfrontalières, où la traçabilité et la preuve des opérations sont essentielles.

Par exemple, elle permettrait de suivre de manière fiable l'origine et le parcours des produits agroalimentaires, d'optimiser les chaînes d'approvisionnement et de sécuriser les transactions commerciales internationales.

Cependant, malgré son potentiel, l'adoption de la blockchain au Maroc se heurte à des obstacles juridiques et réglementaires significatifs. L'absence de reconnaissance explicite de cette technologie dans le droit national crée des incertitudes sur plusieurs points cruciaux.

La recevabilité des preuves issues d'une blockchain devant les tribunaux reste ambiguë, la validité juridique des contrats intelligents (smart contracts) n'est pas clairement établie, et la responsabilité en cas d'erreur ou de dysfonctionnement inscrit dans la chaîne n'est pas encadrée. Ces lacunes peuvent freiner l'adoption de la technologie par les entreprises et limiter l'exploitation de ses avantages pour la transparence et la sécurisation des transactions.

Ainsi, si la blockchain représente un outil prometteur pour renforcer la traçabilité et la confiance dans les échanges, son déploiement effectif au Maroc nécessitera un cadre juridique clair et adapté, ainsi qu'une sensibilisation des acteurs économiques aux enjeux et limites de cette innovation.

1.3. Les apports économiques et organisationnels

1.3.1. Efficacité, rapidité et réduction des coûts

Les entreprises ayant engagé un processus de digitalisation constatent des améliorations significatives dans leur fonctionnement organisationnel. La gestion du temps s'en trouve optimisée, grâce à l'automatisation des tâches répétitives et à la simplification des procédures

internes, ce qui permet aux collaborateurs de se concentrer sur des activités à plus forte valeur ajoutée.

Par ailleurs, la digitalisation contribue à une meilleure qualité de service, en réduisant les délais de réponse aux clients et en limitant les erreurs liées au traitement manuel des informations.

Sur le plan économique, plusieurs études institutionnelles montrent que l'adoption de solutions numériques peut réduire de 30 à 50 % les coûts internes associés au traitement des documents, à la gestion administrative et à la coordination des processus. Ces économies résultent notamment de la diminution des ressources consacrées à la manipulation papier, de la réduction des déplacements physiques et de l'optimisation des flux d'information.

En outre, la digitalisation favorise une plus grande flexibilité organisationnelle, permettant aux entreprises de s'adapter rapidement aux fluctuations de la demande et aux changements réglementaires. Elle facilite également la collecte et l'analyse des données, offrant aux dirigeants des outils décisionnels plus précis et rapides.

L'impact combiné de ces gains d'efficacité et de ces réductions de coûts contribue à renforcer la compétitivité des entreprises, tant sur le marché national qu'international, et à stimuler l'innovation dans leurs pratiques commerciales.

1.3.2. Transparence et confiance économique

La digitalisation contribue significativement à renforcer la confiance entre les différents acteurs économiques. La traçabilité des opérations permet de suivre chaque transaction de manière précise et sécurisée, réduisant ainsi les risques de fraudes ou de litiges.

Les engagements contractuels sont mieux documentés et les preuves plus facilement accessibles, ce qui simplifie le règlement des différends et renforce la sécurité juridique des transactions.

Cette transparence accrue favorise également un climat de confiance propice aux investissements et aux partenariats commerciaux. Les entreprises et les administrations peuvent interagir avec plus de sérénité, sachant que les informations sont vérifiables et que les processus sont moins susceptibles de manipulations ou d'erreurs.

En conséquence, la digitalisation ne se limite pas à un gain d'efficacité organisationnelle, elle devient un vecteur de crédibilité et de stabilité pour l'ensemble de l'écosystème économique.

1.3.3. Obstacles et disparités régionales

Malgré ses avantages indéniables, la digitalisation rencontre encore des freins importants, notamment liés à la fracture numérique.

Dans de nombreuses zones rurales ou marginalisées, l'accès aux technologies reste limité, ce qui exclut certaines populations et entreprises des bénéfices de la transformation numérique.

Par ailleurs, le manque de compétences numériques constitue un obstacle majeur, les petites et moyennes entreprises (PME) éprouvant souvent des difficultés à intégrer efficacement les outils digitaux dans leurs processus.

La capacité d'investissement reste également inégale : alors que les grandes entreprises peuvent financer des infrastructures et des logiciels sophistiqués, les PME et les structures locales peinent à suivre le rythme.

Les disparités dans les infrastructures, telles que la couverture Internet, l'électricité fiable ou les services cloud accessibles, accentuent encore ces écarts régionaux. Ces limites soulignent la nécessité de politiques publiques ciblées et de programmes d'accompagnement pour réduire les inégalités, favoriser l'inclusion numérique et assurer que la digitalisation bénéficie à l'ensemble du territoire.

2. Sécurité juridique des transactions numériques : enjeux, défis et perspectives

La sécurité juridique constitue un pilier central du développement du commerce électronique, car elle garantit la prévisibilité des règles applicables, la fiabilité des preuves et la protection des droits des parties. C'est dans cette optique que la loi n°43-20 relative aux services de confiance pour les transactions électroniques a été adoptée.

Dans un environnement numérique marqué par la rapidité des échanges, la multiplication des prestataires techniques et l'usage croissant d'outils d'automatisation, les risques juridiques se diversifient et se complexifient.

Au Maroc, malgré des avancées perceptibles, plusieurs vulnérabilités persistent et nécessitent une analyse approfondie.

2.1. Protection des parties et cybersécurité

2.1.1. Authenticité, intégrité et preuve électronique

La validité juridique d'une transaction numérique repose d'abord sur la capacité à démontrer que le document électronique n'a pas été altéré et qu'il provient bien de son auteur. En théorie, les mécanismes cryptographiques, l'horodatage, les certificats électroniques, les journaux de connexion et les métadonnées constituent un arsenal robuste permettant d'établir la preuve.

Cependant, la pratique révèle plusieurs limites.

D'une part, les opérateurs économiques ne disposent pas toujours des outils techniques adéquats pour assurer l'archivage probant, ce qui fragilise la conservation de la preuve à long terme.

D'autre part, la jurisprudence marocaine demeure embryonnaire sur l'évaluation de la fiabilité des traces numériques. Les juges se réfèrent encore principalement au support papier et adoptent une approche prudente, laissant planer une incertitude quant à la valeur probante de certains fichiers ou logs en cas de contentieux complexe.

La doctrine appelle ainsi à une clarification normative et à une formation renforcée des magistrats afin d'assurer une interprétation homogène des preuves électroniques, notamment celles issues des plateformes privées ou de systèmes automatisés comme les ERP.

2.1.2. Confidentialité et responsabilité en cas d'incident

Dans un contexte marqué par l'intensification des cybermenaces (telles que les ransomwares, les injections malveillantes, le phishing sophistiqué ou encore les attaques par déni de service) la protection de la confidentialité des données s'impose comme un impératif majeur.

Les entreprises, et en particulier les PME, rencontrent encore des difficultés à mettre en place des dispositifs de cybersécurité conformes aux standards internationaux.

La question de la responsabilité en cas d'incident demeure dès lors particulièrement complexe. En pratique, les contrats conclus entre les entreprises et leurs prestataires techniques, qu'il s'agisse d'hébergeurs, de plateformes, de fournisseurs de services cloud ou encore d'émetteurs de certificats électroniques, ne prévoient que très rarement des clauses détaillant clairement les obligations de sécurité, les modalités de notification des violations, la répartition des responsabilités ou encore les règles relatives à la conservation des journaux techniques.

Cette insuffisance contractuelle accroît la vulnérabilité juridique des opérateurs économiques. Par ailleurs, contrairement à l'approche retenue par le RGPD, la loi 09-08 n'instaure pas d'obligation générale de notification des violations de données, ce qui limite considérablement la traçabilité des incidents et complique leur gestion efficace.

2.1.3. Rôle des prestataires de services électroniques

Les prestataires de services électroniques jouent un rôle essentiel dans l'écosystème numérique en fournissant l'infrastructure nécessaire aux transactions en ligne, qu'il s'agisse de la certification électronique, de la gestion des serveurs, des systèmes de paiement, des identifiants sécurisés, des services cloud ou encore des réseaux de télécommunication.

Malgré cette centralité, leur responsabilité demeure fragmentée entre différents cadres juridiques sectoriels, notamment ceux de l'ANRT, de Bank Al-Maghrib ou encore du régime applicable aux marchés publics.

Cette absence d'un dispositif homogène entraîne un déficit de contrôle quant à la qualité des certificats délivrés, complique l'évaluation de la fiabilité d'un prestataire par les entreprises et limite la transparence relative aux audits de sécurité réalisés.

L'instauration d'un système de qualification unifié, inspiré du modèle européen eIDAS, apparaît ainsi indispensable pour renforcer la sécurité des services fournis et consolider la confiance des usagers dans les transactions numériques.

2.2. Limites structurelles et défis juridiques

2.2.1. Fragmentation normative et disparités d'application

Le cadre juridique marocain applicable au numérique s'est construit par l'addition progressive de lois sectorielles adoptées à des périodes différentes, telles que la loi 53-05, la loi 09-08, les règles de Bank Al-Maghrib relatives aux paiements, les directives de l'ANRT ou encore certaines dispositions du Code de commerce. Si cette architecture témoigne d'une volonté d'encadrer un domaine en constante évolution, elle souffre néanmoins d'un manque de cohérence interne.

Plusieurs difficultés en résultent, notamment des contradictions entre certains textes, l'absence d'un socle commun définissant clairement les responsabilités numériques ou encore un déficit

de coordination institutionnelle entre la CNDP, l'ANRT, Bank Al-Maghrib et le ministère du Commerce.

Cette fragmentation affaiblit la prévisibilité du droit et rend son interprétation particulièrement complexe pour les entreprises, en particulier pour les acteurs émergents tels que les fintechs ou les start-up spécialisées dans la blockchain, qui peinent à identifier les obligations précises qui leur sont applicables.

2.2.2. Risques de fraude et contentieux

La digitalisation ouvre de nombreuses opportunités pour les entreprises, mais elle s'accompagne également d'une intensification des risques de fraude, qu'il s'agisse de faux sites, d'usurpation d'identité, de manipulation de systèmes informatiques ou de détournement de données bancaires.

Les tribunaux marocains sont désormais confrontés à des litiges d'un type nouveau, caractérisés par une dispersion des responsabilités et une fragmentation des éléments de preuve. Plusieurs difficultés se posent, notamment l'attribution complexe d'une action à un auteur en raison de l'anonymat technique, la multiplication de contrats numériques impliquant une pluralité de prestataires, ou encore la nécessité de recourir à des expertises techniques lourdes et onéreuses.

À cela s'ajoute l'insuffisante spécialisation des juridictions en matière numérique, qui limite parfois la compréhension des enjeux techniques sous-jacents.

Ces défis sont aggravés par la survenance d'erreurs algorithmiques au sein des ERP ou des outils d'automatisation, susceptibles de générer des dommages contractuels dont l'origine exacte n'est pas toujours identifiable, ce qui complique davantage l'établissement de la responsabilité.

2.2.3. Transactions internationales, conflits de lois et compétence

Les opérations transfrontalières posent des défis juridiques et pratiques majeurs pour les entreprises et les consommateurs marocains.

Dans un environnement dominé par des plateformes internationales telles qu'Amazon, Alibaba ou les réseaux mondiaux de paiement, il devient particulièrement complexe de déterminer la loi applicable, la compétence judiciaire et les modalités d'exécution des décisions en cas de litige.

Les transactions numériques effectuées à l'international soulèvent plusieurs questions cruciales. La reconnaissance des signatures électroniques étrangères n'est pas systématiquement assurée, ce qui peut compromettre la validité juridique des documents échangés.

De même, la conclusion de contrats sur des serveurs situés à l'étranger pose des interrogations sur la loi applicable et sur la portée des clauses de juridiction incluses dans ces contrats.

Les consommateurs et les PME marocaines peuvent ainsi se retrouver désavantagés face à des acteurs étrangers, notamment lorsqu'il s'agit de faire valoir leurs droits ou d'obtenir réparation.

Ces défis mettent en évidence l'importance d'une harmonisation normative plus ambitieuse, tant au niveau national qu'international.

La mise en place de règles claires sur la reconnaissance des signatures électroniques étrangères, la validité des contrats internationaux et la compatibilité des clauses de compétence avec le droit marocain est essentielle pour sécuriser les transactions numériques transfrontalières. Sans un cadre juridique adapté, les litiges restent difficiles à résoudre et le potentiel économique du commerce électronique international demeure partiellement exploité pour les acteurs marocains.

2.3. Synthèse des travaux antérieurs

Les travaux examinés convergent vers une conclusion claire : si la digitalisation contribue indéniablement à l'amélioration de l'efficacité économique, ses effets positifs ne peuvent pleinement se matérialiser que si elle s'accompagne d'un cadre juridique solide et d'une gouvernance cohérente.

Les études publiées dans la Revue CCA, la Revue Belge et la RFEM mettent en évidence plusieurs constats essentiels. Elles montrent que la confiance des acteurs économiques dépend directement de la maîtrise des risques numériques, que l'efficacité de la certification électronique est étroitement liée à un encadrement strict des prestataires, et que la formation des acteurs économiques et juridiques constitue un facteur déterminant pour assurer la conformité et la sécurité des transactions.

Ces analyses confirment que la sécurité juridique doit être placée au centre de toute stratégie de digitalisation et ouvrent la voie à des perspectives de réformes structurantes pour renforcer la confiance numérique et garantir la fiabilité des échanges électroniques.

3. Perspectives pour renforcer la sécurité juridique au Maroc

Les perspectives de réforme doivent être envisagées de manière intégrée, en combinant modernisation normative, renforcement institutionnel, montée en compétence des acteurs et coopération internationale.

L'objectif est de garantir un environnement numérique sécurisé, conforme aux standards internationaux et favorable à l'innovation.

3.1. Modernisation législative

L'adaptation de la loi 53-05 apparaît aujourd'hui indispensable afin de prendre en compte les avancées technologiques des vingt dernières années et de répondre aux besoins croissants du commerce numérique.

Cette modernisation pourrait inclure un alignement sur les exigences du règlement européen eIDAS concernant l'identification électronique et la qualification des prestataires, ainsi qu'une reconnaissance juridique explicite de la blockchain et des contrats intelligents, notamment pour ce qui concerne leur valeur probatoire et la détermination de la responsabilité.

Par ailleurs, il serait essentiel de clarifier le régime applicable aux traces numériques, à l'horodatage et à l'archivage électronique à valeur probante, tout en introduisant des obligations spécifiques en matière de cybersécurité pour les entreprises manipulant des données sensibles ou exploitant des systèmes critiques.

Une refonte partielle de la loi 09-08 permettrait également d'intégrer des mécanismes de notification des incidents, de portabilité des données, de consentement renforcé et de sanctions dissuasives. Une révision globale de l'ensemble de ces textes permettrait de combler les lacunes existantes et de garantir une cohérence normative.

3.2. Renforcement institutionnel

Le Maroc dispose de plusieurs institutions clés pour encadrer le numérique, mais leurs moyens et prérogatives demeurent insuffisants face à l'ampleur des enjeux.

Il apparaît nécessaire de renforcer les compétences techniques et financières de la CNDP et de l'ANRT, tout en institutionnalisant un mécanisme permanent de coordination entre la CNDP, l'ANRT, Bank Al-Maghrib et le ministère du Commerce.

La création d'une Agence nationale de cybersécurité, dotée de pouvoirs d'audit, de contrôle, de certification et d'alerte, constituerait un atout majeur pour sécuriser les échanges numériques.

En complément, le développement de centres régionaux d'accompagnement pour les PME, offrant un soutien technique et juridique, permettrait d'accélérer la transition numérique et de réduire les risques associés aux pratiques digitales.

3.3. Développement des compétences

La formation représente un levier fondamental pour assurer l'efficacité de la justice et la sécurité de l'usage des outils numériques. Il est essentiel de prévoir une formation continue des juges sur la preuve électronique, la cybersécurité, la blockchain et les contrats intelligents.

De même, le renforcement des programmes universitaires sur le droit du numérique et la conformité réglementaire, ainsi que la formation des avocats, notaires et experts-comptables aux enjeux du digital, constituent des priorités.

La mise en place d'unités spécialisées au sein de la police judiciaire et des juridictions pour traiter les contentieux numériques permettrait de mieux appréhender les litiges technologiques. Enfin, il est indispensable de sensibiliser les chefs d'entreprise aux risques de cyberattaques et à la nécessité de respecter la loi 09-08 afin de renforcer la conformité et la sécurité des transactions.

3.4. Coopération internationale

La digitalisation dépassant les frontières nationales, le Maroc doit intensifier sa coopération avec l'Union européenne afin d'harmoniser les règles relatives à l'identification numérique, à la signature électronique et à la protection des données.

Il est également essentiel de participer activement aux travaux de la CNUDCI portant sur le commerce électronique et les documents électroniques transférables, tout en renforçant la coopération judiciaire internationale pour faciliter l'exécution des décisions en matière numérique.

Parallèlement, le pays peut s'inspirer des expériences africaines en matière d'identité numérique, de plateformes gouvernementales et de cybersécurité. Cette ouverture et cette collaboration internationales constituent des vecteurs majeurs de modernisation juridique et de consolidation de la confiance numérique.

3.5. Promotion de solutions innovantes

L'innovation demeure un moteur central de la compétitivité économique et juridique.

Il convient de promouvoir l'usage de la blockchain pour la traçabilité logistique, la certification documentaire et la lutte contre la fraude, tout en favorisant l'adoption de l'intelligence artificielle dans les procédures de contrôle, la gestion contractuelle, la détection d'anomalies et l'aide à la décision.

Les systèmes d'authentification biométrique, conformes aux standards de protection des données, ainsi que la mise en place de certificats électroniques avancés pour les acteurs économiques sensibles, doivent être encouragés.

Enfin, le soutien aux fintechs et aux start-up juridiques (legaltech) permettra de développer des solutions de conformité automatisée et de renforcer la sécurité et l'efficacité des transactions numériques.

Conclusion

En conclusion, la digitalisation des transactions commerciales représente un levier stratégique essentiel pour la modernisation économique du Maroc. Elle permet d'améliorer l'efficacité opérationnelle des entreprises, de renforcer la transparence des échanges et d'ouvrir de nouvelles opportunités tant sur le marché national qu'international.

Cependant, pour que ce potentiel se concrétise pleinement, il est indispensable de surmonter plusieurs défis juridiques et institutionnels persistants.

La fragmentation normative complique la lisibilité et l'application cohérente des règles, tandis que la vulnérabilité aux cyberattaques expose les acteurs économiques à des risques importants. La responsabilité des prestataires de services numériques reste encore incertaine, et la culture de conformité au sein des entreprises, en particulier des PME, demeure insuffisante.

Le Maroc se doit donc d'adopter une stratégie intégrée et ambitieuse, combinant harmonisation législative, renforcement des institutions de régulation et de contrôle, montée en compétences numériques des acteurs économiques, et renforcement de la coopération internationale.

Le développement et l'adoption de solutions technologiques innovantes, lorsqu'elles sont encadrées par un cadre juridique clair et sécurisé, contribueront à instaurer un climat de confiance numérique indispensable. Cette confiance constitue, en définitive, une condition sine qua non pour soutenir durablement la croissance du commerce électronique et favoriser l'émergence d'un écosystème économique moderne, inclusif et résilient.

Bibliographie

Ouvrages et articles

Adler, P. (2002). Market, hierarchy and trust. *Organization Science*.

Azevedo, S., Carvalho, H., & Cruz-Machado, V. (2012). Lean and green: the role of digitalization. *Journal of Operations Management*.

Benkirane, F. (2020). La force probante de la signature électronique. *Revue Marocaine de Droit*.

Berrada, L. (2022). *Blockchain et transactions commerciales*. Éditions Universitaires.

Galeazzo, A., Farias, L., & Duarte, M. (2013). Technology and organizational performance. *European Management Journal*.

Kovilage, S. (2020). Digital trust and cybersecurity. *Revue Belge*.

Schuller, T., Baron, S., & Fields, G. (2000). Trust in digital environments. *Harvard Business Review*.

Tahiri, K. (2021). La certification électronique au Maroc. *Revue CCA*.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution*. Penguin Books.

UNCTAD (2022). *Digital Economy Report*.

Textes législatifs

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

Loi n° 09-08 sur la protection des données personnelles.

Loi n°43-20 relative aux services de confiance pour les transactions électroniques

Code de commerce marocain.

Règlement européen eIDAS n° 910/2014.

Rapports officiels

CNDP, *Rapports annuels 2018–2023*.

Bank Al-Maghrib, *Rapport sur les paiements électroniques*.

Ministère de l'Industrie et du Commerce, *Digitalisation des entreprises marocaines*.