

Electronic Commercial Contracts in Saudi Arabia: Legal and Regulatory Challenges

¹Duaa Hijazi; ² Mona Omran; ³ Emran Alzubi and ⁴ Renad Aldmour

¹literature , Law Department, Faculty of Business Administration, Northern Border University, Arar, Saudi Arabia.

² Associated professor, Law Department, Faculty of Business Administration, Northern Border University, Arar, Saudi Arabia.

³ literature , Law Department, Faculty of Business Administration, Northern Border University, Arar, Saudi Arabia.

⁴ literature , Law Department, Faculty of Business Administration, Northern Border University, Arar, Saudi Arabia.

Abstract:- This study explores the legal and regulatory challenges associated with electronic commercial contracts in Saudi Arabia. As e-commerce grows globally, the Kingdom has witnessed rapid changes in commercial practices, necessitating a robust legal framework to regulate electronic contracts. The paper examines the historical development of e-commerce in Saudi Arabia, the regulatory framework governing electronic contracts, and the challenges that arise from their enforcement. Key issues include the compatibility of electronic transactions with traditional legal principles, the recognition of electronic signatures, and cybersecurity concerns that impact the validity and enforceability of these contracts. Additionally, the paper compares Saudi Arabia's legal framework with international standards, highlighting gaps that hinder the effective regulation of electronic commerce in the Kingdom. Recommendations for reform include harmonizing local laws with global best practices and enhancing cybersecurity measures to foster trust in electronic transactions. The study emphasizes the need for legal clarity to support the growth of e-commerce while protecting both businesses and consumers in the digital age.

Keywords:- *Electronic Contracts, E-Commerce, Legal Challenges, Cybersecurity, Electronic Signatures.*

I. INTRODUCTION

Never in the history of man have commercial contracts occupied so vital a part of our daily lives as they do today. Due to the significant evolution in commercial practices, the role played by electronic contracts has become much more significant in recent years. Today, people are spending most of their time online dealing with e-commerce. Not a business day passes without hearing of at least one deal having been concluded over the internet. The internet and other information and communication media have, however, encountered some obstacles while offering solutions to these problems. One such problem is legal issues. (Khan et al.2021)

It is therefore no surprise that, given Saudi Arabia's business and economic climate, a thorough discussion of the different aspects of electronic commercial contracts has merit. Traditionally, most people in business are reluctant to change the methods that have served their forefathers well. In recent years, however, the rapid growth of e-commerce, as a substitute for the traditional way of doing business, has left many vacant spaces in the field of commercial contracts. Recently, many practitioners have started awakening to the notion that e-contracts are here to stay mainly due to the fact that e-commerce is increasingly popular with the business community. So, the most important question is how we in Saudi Arabia are going to face the challenges arising from modern practices? This is the concern that we will discuss in depth throughout this essay. (Stepper and Kurth2020)

In this essay, we will discuss electronic commercial contracts, the historical background of traditional commercial contracts, electronic commercial contracts in practice, methods to form an electronic commercial contract, and finally, we will examine the legal challenges of electronic commercial contracts.

This discussion is relevant and should be taken seriously because the drafting, implementation, and consistent aim to improve such laws will have implications for the business environment in Saudi Arabia. Their failure to pay attention to such a fundamental change will stifle vital economic development in the Kingdom of Saudi Arabia.

In light of these reflections detailed above, this essay has the following aims: A. To discuss the definition of traditional commercial paper; B. To identify in brief the historical background of traditional commercial contract paper; C. To define e-commerce; D. To identify the place of electronic contracting in e-commerce; E. To identify the methods for forming an electronic commercial contract; F. To consider the problems of electronic commercial contracts in practice; G. To identify the legal and regulatory challenges of electronic commercial contracts.

II. HISTORICAL DEVELOPMENT OF ELECTRONIC COMMERCE IN SAUDI ARABIA

E-commerce in Saudi Arabia has a relatively short history. It is believed to date to 1997, when the concept of e-commerce as we know it was marketed to the public as being the result of the internet. Saudi authorities, specifically the Communication and Information Technology Commission, have been involved in setting up the internet in the country. The CITC is the regulatory authority responsible for regulating the information technology and telecommunications sectors in the Kingdom. (AlSelami2021)

A few of the milestones in the early stages of e-commerce development in Saudi Arabia include: In 1999, the E-Government Programme was launched. In 2001, the first conference on e-commerce and e-government in Saudi Arabia was hosted by the Saudi Ministry of Industry. Saudi e-commerce companies were extremely active from 2000 to 2001 and had a strong presence in the Saudi market. In March 2001, Saudi Arabia passed the e-commerce law, which regulates electronic, commercial, and related transactions. Prior to that legislation, there was no specific law governing e-commerce-related activities. Saudi e-commerce platforms have been more advanced in terms of IT equipment and infrastructure, while the low level of e-commerce penetration meant that the Saudi market was still attractive to global companies. There are high levels of productivity in the ICT and e-commerce sectors in Saudi Arabia. Culturally, in remote areas of the country, face-to-face transactions are preferred, which has hindered the growth of electronic commerce in Saudi Arabia. The slow speed of the internet and expensive tariffs for broadband connections are barriers to e-commerce activity. In November 2009, 10 of the most influential Saudi e-commerce websites were listed in a prominent section of a major newspaper in Saudi Arabia at the time. (Alshathri, 2022)

III. LEGAL FRAMEWORK FOR ELECTRONIC COMMERCIAL CONTRACTS

Electronic commercial contracts can be governed by a number of laws and ensnared in a thicket of legal rules and regulations, which may necessitate a multitude of actions and obligations for the contracting parties. The existence of suitable electronic commercial laws and the legal environment play a critical and essential role in the growth and success of international and regional e-commerce transactions. The need for a uniform set of laws may protect and facilitate the activities related to the establishment and enforcement of electronic commercial contracts. National e-commerce and electronic transactions laws and regulations should be in harmony with those of the international laws. Creating a favorable regulatory e-commerce environment can result in attracting investment and support for the growth, innovation, and development of e-commerce activities. Legislative

enunciations will be broken down in detail based on their relevance to electronic contracts. Regulation of e-commerce in general applies to electronic communications. (Bernstein, 2022)

➤ *Rights and Obligations in Electronic Contracts: (Barnett & Oman, 2021)*

The rights and obligations of the parties to an electronic contract are determined by the internal law applicable to the electronic transaction, which provides that electronic transactions shall not be effective unless they comply with the requirements of the law applicable to the same, and they shall be invalid as per the provisions of this law. The practical touchstone of these general principles lies in the available governmental, judicial, and quasi-judicial remedies that allow contracting parties to enforce their rights and claim remedies in the contractual and extra-contractual failings of their e-commerce business partners and other parties or institutions with whom they have or may have any potential confrontation or dispute. It is the regulatory authorities' duty to assure such compliance in a proactive way and also to investigate and enforce it. Regulatory authorities should aim to help the relevant parties by suggesting alternative regulations, assisting parties who dispute issues that have not been clarified in relevant laws by stipulating relief methods, or by accommodating the means of alternative settlements. In an attempt to create a clearer picture of the applicable rules of law, a number of judicial decisions have been issued. An electronic or email exchange of an offer and acceptance will form a valid contract, and the exchange is deemed to be taking place at the time the dispatch of the e-offer is being received.

➤ *Applicable Laws and Regulations*

The two primary legislative instruments governing e-commerce in the Kingdom of Saudi Arabia are the E-commerce Law and the E-commerce Implementing Regulations. The Council of Senior Islamic Scholars of Saudi Arabia resolution was published in the Official Gazette, confirming that the E-commerce Law did not contravene Islamic shari'a and that it is fully compatible with its provisions. With respect to conventional commercial transactions, Saudi Arabian law will facilitate the regulation of e-commerce. The Kingdom of Saudi Arabia is a signatory to various international agreements addressing trade-related aspects of IP rights, which are relevant in the context of e-commerce. The Civil Code, as well as the Commercial Code, govern commercial activities, including contracts, regardless of the medium of contract formation, and the rights and obligations arising therefrom. These codified laws are supported by principles of shari'a and are also subject to the interpretation of religious edicts issued by the Council of Senior Islamic Scholars and fatwas issued by similar councils. (D et al.2021)

Accordingly, various regulatory frameworks are relevant to understanding e-commerce laws in the Kingdom. In addition, the Saudi Arabian Communications and Information Technology Commission, which has wide powers to regulate, enforce, and monitor activities in the IT sector, has issued implementing classification guidelines addressing issues such as filtering, compliance, and monitoring. The developments in e-commerce laws in Saudi Arabia take into account various national as well as international laws. In the area of contract law, international conventions and treaties continue to have a significant impact. Laws governing electronic contracts must guarantee legal certainty and transparency in order to promote trust in the e-commerce context. Such laws must also prevent and resolve legal obstacles. However, it is noted that national laws of states today are moving at uneven rates to harmonize local laws with these agreed international principles. Consequently, the legal environment in different states, apart from reflecting variations of local legal traditions and cultural norms, is affected by global pressures towards harmonization. In the case of Saudi Arabia, the international aspects of the topic are especially instructive because the country's legal regime as a civil law jurisdiction has a large statutory influence in the form of law. Furthermore, globalization pressures, combined with the relatively advanced nature of the Kingdom's E-commerce Law, dictate that an understanding of applicable international and locally influential regional agreements is essential to evaluating the legal anchorage of electronic commercial contracts in Saudi Arabia. Indeed, it was declared that future international e-commerce trade will be best served by countries harmonizing national laws that govern electronic commerce. Inasmuch as international principles are increasingly affecting local laws on electronic commerce, these agreements may generally be helpful as practical indicators that many countries follow or look to in the process of domestic regulation. (Sarabdeen, 2023)

➤ *Key Provisions for Electronic Contracts*

The crucial issue in any e-commerce law is the regulation of electronic contracts. Thus, this section highlights some of the major provisions in the framework that are related to regulating commercial and contractual dealings from an e-commerce perspective. In this regard, the Saudi law recognizes that in order to be valid, any digital agreement must include the elements of an offer, acceptance, and consideration in whatever form. The importance of authenticity in electronic commercial transactions is also reflected in the law through stipulations that provide the recognition of a valid electronic signature, which mirror in electronic form the requirements of the formalities of signatures. (Alanzi, 2021)

In an attempt to regulate a fast-growing commercial area, the regulation also stipulates certain mechanisms related to the operation of e-commerce platforms. This includes stipulations regulating the protection of personal information, which reflects the influence of international instruments seen in the

law, the increasing consumer rights protection, and consumer confidence seen in developed and emerging legal systems, as well as the increasing realization of the importance of utilizing personal information for economic and efficiency purposes. The law delegates judicial bodies with the tasks of the interpretation and enforcement of its provisions as mentioned in its general clauses. For instance, the law provides a clear stipulation that unless stated otherwise, the rules and principles regulating paper-based transactions shall apply to ECP. In theory, it is the judicial bodies, and particularly the Cassation Board, who should devise acceptable standards to be followed in identifying the nexus in such transactions. More practically, however, it is important to note that there are very few precedents in relevant cases under the new regime to help ascertain the type or degree of interpretation the judiciary lends to e-commerce law. (Ahdout, 2021)

Although these provisions serve as a good basis to understand the commercial rules governing electronic contracts in the Kingdom of Saudi Arabia, there are several issues that must be borne in mind while analyzing this chapter, which hinder the effective implementation of such provisions in actual practice, particularly in the Saudi case. For instance, in practice, it requires 'a specific electronic signature' without providing a clear definition of what this means. Moreover, it has to almost always state that 'unless otherwise provided in a contract, an offer may be revoked if the revocation reaches the offeree before the offeree sends an acceptance.' The revocation of the offer reaches the offeree when he is notified of the revocation in line with the usual manner of communication between such parties or when his attention is given to the revocation. This poses an enormous challenge for e-commerce contracts. In short, the practical realities of e-commerce and developing business make complying with such stipulations difficult and impose a heavy burden of due diligence upon the contracting parties. It is precisely to get a grasp of such practical operationalities of electronic contracts and to provide guidelines on how to handle them that this chapter delves into the theoretical formulation of the law. (Zheng et al.2020)

IV. ENFORCEMENT OF ELECTRONIC CONTRACTS IN SAUDI ARABIA

➤ *Enforcement of Electronic Contracts*

A. Basics of E-Contract Enforcement E-contracts performed in electronic transactions are generally classified based on the agreement of the parties in terms of the intention to be legally bound. That is, though information systems and the internet are the operational mediums as well as entities, the foundation of e-contract law is essentially the law of contract. The enforceability of electronic data is not any different from that of paper data, as both are considered to have the same legal nature. Data created partly or wholly with electronic or digital tools are regarded as electronic counterparts of their manual equivalents. Electronic agreements are enforceable against contracting parties who enter into contracts by

agreeing on similar electronic communication. The effectiveness of enforcement, with the courts, tribunals, or arbitral bodies, is considered more important as it lays down the foundation for increasing the utilization of e-commerce. New techniques in encryption and other security devices can provide protection to facilitate the acceptance of electronic commercial contracts and their electronic signatures. Before the successful use and reliance on e-contracts in day-to-day commercial transactions, all the above issues must be addressed and the laws related to electronic agreements must be properly implemented. (Viljoen, 2021)

B. Factors Influencing the Function of the E-Enforcement System The more awareness there is about orders and implementation in electronic contracts, the fewer disputes and conflicts there will be. This early prevention measure should gladly be attended to by the promoters and early users of e-agreements, especially e-merchandising. The use of the 'track and trace' clause in the present situation of e-commerce should be more meaningful, bearing in mind that most contracts, such as simple contracts for sale, do not deal with rights and obligations at the commencement of the transaction but operate during the currency of the transaction. All contracts that are either to be negotiated or are subject to status can first of all be reduced to provide an automated solution similar to the 'track and trace' system. A prospective juridical measure in addressing the issues of jurisdiction and choice of forum in electronic agreements would be to insist that all contracting parties choose to have jurisdiction and law that provide legal clarification for the enforcement of electronic obligations. Given the inevitable international aspect of electronic commerce, problems of jurisdiction and applicable law are identified as major impediments. Valid legal mechanisms and enforcement paradigms should be in place to offer redress for any nonperformance. It is the legitimacy of the creation of e-obligations that results in the legitimization of any redress. The gravamen, therefore, in all discussions on enforcement remains the compatibility of the informal nature of ordering and ordering mechanisms with the enactment through the medium of e-contracts. (Svensson-Hoglund et al.2021)

➤ *Recognition of Electronic Signatures*

Electronic signatures are generally recognized under Saudi law through two aspects. First, an electronic statement, including approvals, can be accepted through electronic communication and be binding as long as the communication complies with legal criteria for it. The second aspect deals with the legal and regulatory recognition of specific categories of electronic signatures like electronic signature certificates and digital signatures, including their various degrees of technological or semi-technological security, known as advanced electronic signatures, in relevant provisions of the E-C Transactions Law. (Atim, 2020)

Such recognition is essential for making electronic signatures or a category of them reliable, in view of digital evidence, thus increasing the legitimacy of paperless electronic contracts and e-governance driven by secure digital interactions. Legally, the adoption of such a stance is expected to lend a strong reason for the judiciary to support digital efficiency and move away from the emphasis on authorship and signed writings. From the perspective of international best and practical standards, electronic signature regulations would offer these standards based on local needs, such as increased reliance on JIT contracts, mixed with a robust emphasis on articulating the modalities of the required electronic technology security. Electronic signature regulation propounds certain circumstances under which an electronic signature has a predetermined security level, making it reliable versus other types of electronic signatures. These regulations often balance factors like convenience of use and technological propagation against stronger security needs. They often establish the functions of certification authorities and their roles and liability. Enforcement is imposed by a public regulatory authority. International standards and best practices on global electronic signatures, including electronic signature certificates and advanced electronic signatures, consist of parts of the Model Law on Electronic Signatures and the Harmonized Trustworthy Legal Infrastructures Guidelines. Such guidelines recognize that states adopting them promote the approach of trusted electronic signature infrastructures with sound economic reasons. These approaches adopt basic labeling systems for verifying signatures in electronic form accompanied by a signature-creation data validation system for the detection of forgery. The effectiveness dimension of these bodies and the certificates issued are enhanced through both the track record of CA bodies and soft or, in some cases, legal liability. On a global level, electronic signatures, including advanced electronic signatures and electronic signature certificates, are recognized under the e-Commerce, e-Authentication, and e-Government Conventions. These conventions reinforce the substantive rules on the formation and conclusion of contracts through electronic signatures as binding. In contrast, the terms and conditions for respecting an electronic signature are defined in practical terms as a form of electronic evidence towards nationals and across borders. In this regard, a Western electronic signature can be accepted by a Saudi national on purely practical and/or regulatory grounds based on reliability assessments emanating from a bilateral trust agreement of PKI supervisory authorities with CAs of the exporting state. Alternatively, it can be assessed by Saudi nationals based on a basket of quality indicators of electronic signatures' security levels. (Pandora & Makarim, 2022)(ESCAP, 2020)(Pasadilla, 2020)

➤ *Admissibility of Electronic Evidence*

In any judicial proceedings, the function of evidence is to establish the existence or nonexistence of a fact in order to prove or disprove a matter in dispute. This subsection discusses the admissibility of electronic evidence in judicial proceedings in relation to electronic contracts. Admissibility relates to the conditions under which electronic evidence should be collected and presented to a court so that it has the desired value and serves its function as evidence in court. The starting point is that electronic evidence is only admitted into a judicial proceeding if it meets the prescribed criteria and standards, and is valid and reliable, as required by the principles of evidence. In the absence of such criteria-specific laws and practices regarding electronic evidence collection and presentation, scrutiny and evaluation in a court of law may raise questions as to the validity and reliability of the proof. (Reiling, 2020)

Common formats of electronic evidence may include the historical databases of electronic contracts, internet service provider logs, and logs of servers or network devices. Certain laws and investment contracts may prescribe that an electronic contract can become evidence and may be adduced in courts. Despite this, a potential challenge is that this evidence might be marred by claims of tampering, lack of authenticity, and lack of evidence source integrity being brought before the court. Amendments may be added to evidence logs because they are typically managed by custodians who have an interest in the case in question. The law of evidence in many jurisdictions may stipulate the requirements for admitting an electronic data log as evidence. Specifically, electronic data logs must be authentic in the source, and the required party must have control over the data. Following this, the party must have issued the document and the date of the document will have to be proven in court. In cases of international dispute, not abiding by such rules can cause court authorities to disfavor the party presenting electronic evidence. In practice, the data logs collected from electronic devices are generally collected as electronic evidence. However, they will need to undergo several steps to ensure their admissibility and authenticity in court. This is often done using a method known as Digital Forensics. Courts and lawyers are often unaware of these procedures; the primary source of digital forensics regulations is currently considered the global leader for forensic technology and practice. Aligning the collection and presentation of evidence with international laws enhances harmony between parties in international cross-border disputes. (Wu & Zheng, 2020)

V. CHALLENGES AND ISSUES IN ELECTRONIC CONTRACT ENFORCEMENT

➤ *Saudi Commercial Contract Laws - Legal and Regulatory Challenges*

VII. Challenges and Issues Enforcing electronic contracts is beset with many challenges and issues. One major challenge for e-contract enforcement is the transnational character of electronic contracts. The global reach of the internet is such that e-contracts can frequently emanate from several different countries, and as a general rule, electronic transactions are transnational. Another major issue in electronic commercial transactions is the contention of personal jurisdiction. The growing use of electronic transactions by international companies has led to the transnationalism of electronic contracts since electronic commerce is global in nature. Such a situation can also lead to the issue of determining which law will govern the electronic transactions. (Zheng et al.2020)

The trepidation about technology devices, especially their vulnerabilities to security threats, adds to the list of issues. Cybersecurity incidents are dominating the agenda of stakeholders involved in electronic transactions. The increase in cybersecurity threats to electronic transactions for online business is concerning. The surging number of conducted attacks is further complicating the trust issue in electronic online transactions. Undoubtedly, such security threats could lead to significant challenges for present-day electronic transactions. Indeed, the perhaps biggest issue concerning electronically executed contracts is that while the legal framework is well-equipped to safeguard pen and paper contracts, it is unclear if the same rules and regulations will suffice for safeguarding the interests of owners of electronic contracts. Therefore, the electronic forum calls for collaborative measures involving many stakeholders in order to ensure this trust. Undoubtedly, the technology's numerous shortcomings have significantly weakened the trust that both businesses and consumers have in the electronic forum. For instance, failure to adopt a trusted e-signature has in the past led to costly lawsuits. Furthermore, the possibilities of cyber attacks necessitate the use of stringent information and cyber laws and organizational practices that can secure the confidentiality, integrity, and authenticity of information. Inadequacy in this area could equally attract global concerns. The cyber attack involving a significant number of credit card records of customers summed up the issue. (Belwal et al.2021)

➤ *Cross-border Legal Issues*

Enforcing an electronic contract across international boundaries might be quite intricate. The world consists of exclusive legal systems; therefore, the substantive regulations to which parties are likely to adhere can differ in genuine commercial practice. This might be the basis for a jurisdictional contest if a problem with an electronic commercial agreement arises. One way or another, the regulations of more than one authority might be of interest or apply to a cross-border loss. Dissimilarity in regulations across different legal systems may lead to adversarial implications for contract performance. If cross-border electronic obligations are unnegotiated and the other party is seated abroad, the affected party may have legal and practical complexities in taking court decisions abroad. The alternative of a law that applies to a cross-border electronic agreement is not inevitable. The rules of many countries stipulate conflicts following the standards of their own law to determine where they are the most fitting. (Svantesson, 2021)

Conversely, the parties to the agreement might not recognize or prefer to conform to a particular regulation because they anticipate disputes. Given the existing investment by international organizations in creating the technical and legal standards to support global e-commerce, a harmonious regulation is desired. IT adoption might be hindered by differences between legal systems and pronouncements. Some developed countries utilize either a portion of the rules or a treaty to establish contractual relations. The treaty contains an application mode to participate in material appliance reservations. Consequently, the dissimilar substance of national regulation can be reduced. The introduction and execution of information and communications systems are a representation of political will. They signal that there is a determination in governments to create the required legal framework for the growth of electronic commerce. This approach can be employed to advance the universal harmonization process. United efforts should be anticipated between states when dealing with cross-border electronic settlement. As a result, sound execution of regulations and policies is, in many ways, about procedural synergy. (Singh2023)

➤ *Cybersecurity Concerns*

The contracting parties in electronic commerce are exposed to various cybersecurity issues that affect the enforceability of electronic commercial transactions. The number of cybersecurity incidents in electronic commerce is consistently growing. Security vulnerabilities associated with online transactions result from inadequate web security policies related to closed-circuit communication and the risk of data breaches. User privacy, transmission integrity, and message confidentiality are all subject to attack, potentially undermining the logical structure of messages exchanged by the contract parties. Information system breaches, including manipulated terms and contracts as well as holding breached

databases and systems hostage, disrupt the authenticity, integrity, and non-repudiation of electronic records. Common cybersecurity threats that have been identified in e-commerce include hacking, denial of service, malicious software, social engineering, and insider threats. Phishing and identity theft are some of the more common cybersecurity issues in e-commerce that concern both businesses and consumers. (Luo & Choi, 2022)

The legal framework for addressing cybersecurity concerns in electronic transactions is not comprehensive. The legal and regulatory perspective of cybersecurity issues in electronic transactions is discussed in detail. In countries like Saudi Arabia, there are legal and regulatory measures aimed at addressing cybersecurity challenges in electronic transactions. However, these measures apply within each country, and there are no laws or regulations that can be used to combat cross-border cybersecurity issues that may arise in an e-commerce ecosystem. Similarly, a comprehensive approach to addressing electronic contracting issues is yet to be considered. Some recommendations to address cybersecurity challenges in electronic contracting include establishing a more robust cybersecurity legal and regulatory framework. This should be complemented with the establishment of specialized private firms in the field of technical and legal cybersecurity for electronic transactions and dedicated training and awareness programs to increase the level of awareness and clarity of the rules for the stakeholders in the contracting process. Furthermore, continuous communication and cooperation between all parties is fundamental for identifying and responding to future and emerging trends of electronic transactions. In this respect, the role of government bodies progresses to work with the private sector to protect critical electronic infrastructure when addressing cybersecurity challenges. Thus, an integrated approach for cybersecurity challenges that involves both the government and private sector should be available. (Sikder and Allen2023)

VI. COMPARATIVE ANALYSIS WITH INTERNATIONAL STANDARDS

This section discusses Saudi Arabia's electronic commercial contract framework in comparison with international practices and standards. This comparison highlights how the Saudi e-commerce legal framework has deficiencies that need to be addressed to bring it in conformity with effective international commercial practices. Because of its potential to facilitate international trade and investment, contracts in electronic form are facilitated by a large number of international and regional agreements and regulations. There are areas where convergence in these international standards exists. Those e-commerce regulatory regimes authorizing a move from paper to electronic contracting often also stipulate that such electronic commerce will have legal validity, enforceability, and recognition. Any regulatory environment that does not facilitate the enforceability and

acceptance of electronic contracts always creates practical challenges. The Saudi legal framework for electronic contracts confirms a discord with these generally accepted norms. (Algahtani, 2021)

Under international agreements and model laws, specific requirements are laid down for reaching e-conformity or establishing enforceability. The fact that some requirements are laid down, such as the need to meet writing and signature formalities for enforceability, is an admission that in the absence of that requirement, contracts would be unenforceable or of doubtful status. Therefore, the absence of such requirements in the Saudi system is not in line with these internationally accepted norms. The reliance on international standards and best practices provides a roadmap to facilitate legal change to meet these international norms. This could involve abandoning formalistic adherence to past practices such as the need for writing or a signature, for example, in the context of specific exceptions for sales of goods and negotiable instruments. Alternatively, structural impediments noted in the regulatory framework should be addressed. For example, the current legal uncertainty surrounding the evidential status of electronic materials could be navigated through clarifications, so that the sufficiency of electronic contracts to conclusively describe deal terms and constitute a basis of commerce is confirmed. The evocation of these international standards provides a useful frame of reference and benchmark against which to understand the policy options available to remedy existing deficiencies in the legal regime. (Bursztyn et al.2020)

VII. PROPOSED REFORMS AND FUTURE DIRECTIONS

This article has identified clear gaps resulting from the ragged legal framework and the lack of statutory clarity concerning electronic commercial contracts in Saudi Arabia. Hence, a number of amendments and additional actions are proposed in this regard. These recommendations reflect the suitable approaches and international practices that can be implemented as appropriate reforms in the KSA to invigorate the e-commerce environment in favor of its stakeholders. In conclusion, the unsuitability and obscurity of the current e-commerce provisions as prescribed by the Saudi local law affect the general atmosphere for e-commerce compliance. Clearly defined and understandable conditions should be outlined to build a clear and regulated atmosphere for e-contracts, ICT, and e-commerce. Regulatory control and performance standards must be uniformly described in the commercial marketplace for the private and public sectors, thus addressing the legal risk in case of any failure to comply with relevant statutes. As with amendments, education and training must be part of the implementation strategy. Educating people about the convenience of using e-contracts in Saudi Arabia and building systems in their own organizations will help them align with the best approach.

Furthermore, the private sector must engage and collaborate with the appropriate parties to create a legal environment that responsively meets the immediate and future requirements of all e-commerce parties/entities in general, while addressing the indirect risks of the processes themselves. Risks that are directly related to the e-operators. Security and its necessities remain an overriding priority. Ongoing awareness and social collaboration complement appropriate standardization that is in line with international and local trends. These amendments in KSA are therefore in line with international best practices and ensure that the necessary stakeholders' requirements are met. Ensuring all e-signatures and e-authentication are risk-mitigated is tantamount to any electronic transaction.

VIII. CONCLUSION

This paper provides a comprehensive analysis of the barriers that hinder e-commerce development in Saudi Arabia specifically regarding electronic commercial contracts including legal and regulatory challenges. By addressing these challenges, the country could foster a more credible e-commerce market for local and global investors. It is in the best interest of the KSA to ensure that all electronic transactions comply with appropriate regulations in order to avoid potential disputes in e-transactions. When a well-organized legal environment is in place, it recounts trust among consumers and traders in the e-commerce field.

Although Saudi Arabia has a general law on electronic commerce, there is a need to develop clear laws that aim to regulate electronic contracting. By addressing these prospected challenges, the next legal step should detail clear regulations on electronic contracts and their validity within the judicial system and should also include a system for authorized certification service providers that can issue digital signatures. Moreover, Saudi Arabia's judicial and arbitration systems may need to develop systems that can address the probative value of digital evidence and electronic contracts.

Fostering a better e-commerce environment includes developing new legal structures that allow and authorize various electronic contracts within the electronic commercial activity. As a recommendation, alongside developing new laws, the proposed system should align with international standards. Further, the judiciary should be involved in providing new guidelines or enforce novice legislation in a more creative way by going in line with the development of technology. Finally, there is a need to start a comprehensive and concentrated dialogue between these stakeholders in order to communicate problems related to legislation pertaining to e-commerce, which together with technologists, jurists, and legislators should attempt to introduce standards that would provide the legal framework with sophisticated and accurate control of e-commerce by regulating the main axes in e-commerce, including digital signature, regulates the credentials of the parties to the contract. In light of these

nuanced difficulties, this paper paves the way for future research on this topic, focusing on analyzing those laws compatible with the challenges facing virtual currency and the use of blockchains in the e-contract.

REFERENCES

- [1]. Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*, 14, 2901-2925. [springer.com](https://www.springer.com)
- [2]. Stepper, M., & Kurth, D. (2020). Transformation strategies for inner-city retail locations in the face of E-commerce. *Proceedings of the Institution of Civil Engineers-Urban Design and Planning*, 173(5), 159-170. [HTML]
- [3]. AlSelami, F. A. (2021). Strategic Roles of Big Data in Supporting the National Economy & Business Sector in Light of the Vision of the Kingdom of Saudi Arabia 2030. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies*, 12(8), 1-15. [tuengr.com](https://www.tuengr.com)
- [4]. Alshathri, S. A. (2022). Online dispute resolution as a mechanism to enhance consumer trust in e-commerce: how can Saudi Arabian law be improved?. [ncl.ac.uk](https://www.ncl.ac.uk)
- [5]. Bernstein, L. (2022). Merchant law in a merchant court: Rethinking the code's search for immanent business norms. *The Creation and Interpretation of Commercial Law*. [upenn.edu](https://www.upenn.edu)
- [6]. Barnett, R. E. & Oman, N. B. (2021). Contracts: Cases and doctrine. [HTML]
- [7]. D AL-TAYYAR, R. S., Abdullah, A. R. B., Abd Rahman, A., & Ali, M. H. (2021). Challenges and obstacles facing SMEs in the adoption of e-commerce in developing countries; A case of Saudi Arabia. *Studies of Applied Economics*, 39(4). [ual.es](https://www.ual.es)
- [8]. Sarabdeen, J. (2023). Laws on regulatory technology (RegTech) in Saudi Arabia: are they adequate?. *International Journal of Law and Management*. [HTML]
- [9]. Alanzi, A. A. (2021). Saudi procurement system and regulations: Overview of local and international administrative contracts. *Laws*. [mdpi.com](https://www.mdpi.com)
- [10]. Ahdout, Z. P. (2021). Enforcement lawmaking and judicial review. *Harv. L. Rev.*. [HTML]
- [11]. Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, 105, 475-491. [PDF]
- [12]. Viljoen, S. (2021). A relational theory of data governance. *Yale LJ*. [yalelawjournal.org](https://www.yalelawjournal.org)
- [13]. Svensson-Hoglund, S., Richter, J. L., Maitre-Ekern, E., Russell, J. D., Pihlajarinne, T., & Dalhammar, C. (2021). Barriers, enablers and market governance: A review of the policy landscape for repair of consumer electronics in the EU and the US. *Journal of Cleaner Production*, 288, 125488. [sciencedirect.com](https://www.sciencedirect.com)
- [14]. Atim, Z. A. H. (2020). Evidence In The Saudi Electronic Transaction System, A Comparative Study With The Uncitral Model Laws. *J. Legal Ethical & Regul. Isses*. [academia.edu](https://www.academia.edu)
- [15]. Pandora, F. S. & Makarim, E. (2022). Implications Using Electronic Stamp Duty Authentic as Proof of Electronic Documents in Indonesia. [Cepalo. unila.ac.id](https://www.cepalo.unila.ac.id)
- [16]. ESCAP, U. N. (2020). E-commerce provisions in RTAs: Implications for negotiations and capacity building. [unescap.org](https://www.unescap.org)
- [17]. Pasadilla, G. O. (2020). E-commerce provisions in RTAs: Implications for negotiations and capacity building. [econstor.eu](https://www.econstor.eu)
- [18]. Reiling, A. D. (2020). Courts and artificial intelligence. [IJCA. iolr.org](https://www.ijca.iolr.org)
- [19]. Wu, H. & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer law & security review*. [researchgate.net](https://www.researchgate.net)
- [20]. Belwal, R., Al Shibli, R., & Belwal, S. (2021). Consumer protection and electronic commerce in the Sultanate of Oman. *Journal of Information, Communication and Ethics in Society*, 19(1), 38-60. [HTML]
- [21]. Svantesson, D. J. B. (2021). Private international law and the internet. [HTML]
- [22]. Singh, B. (2023). Unleashing Alternative Dispute Resolution (ADR) in Resolving Complex Legal-Technical Issues Arising in Cyberspace Lensing E-Commerce and Intellectual Property: Proliferation of E-Commerce Digital Economy. *Revista Brasileira de Alternative Dispute Resolution-Brazilian Journal of Alternative Dispute Resolution-RBADR*, 5(10), 81-105. [emnuvens.com.br](https://www.emnuvens.com.br)
- [23]. Luo, S. & Choi, T. M. (2022). E-commerce supply chains with considerations of cyber-security: Should governments play a role?. *Production and Operations Management*. [HTML]
- [24]. Sikder, A. S., & Allen, J. (2023). An In-depth Exploration of Emerging Technologies and Ethical Considerations in Cross-border E-commerce: A Comprehensive Analysis of Privacy, Data Protection, Intellectual Property Rights, and Consumer Protection in the context of Bangladesh.: *Technologies and Ethical Considerations in Cross-border E-commerce*. *International Journal of Imminent Science & Technology*, 1(1), 116-137. [ijisnt.com](https://www.ijisnt.com)
- [25]. Algahtani, A. M. (2021). Legal Uncertainty and the Effect of Legal Duality on the Legal System of Saudi Arabia. [HTML]
- [26]. Bursztyn, L., González, A. L., & Yanagizawa-Drott, D. (2020). Misperceived social norms: Women working outside the home in Saudi Arabia. *American economic review*, 110(10), 2997-3029. [uzh.ch](https://www.uzh.ch)