



Electronic Contracts in India: Legal Challenges and Comparative Perspectives

Omendra Singh, Ph.D., Department of Law
Brahmanand PG College, Kanpur, Uttar Pradesh, INDIA

ORIGINAL ARTICLE



Author

Omendra Singh, Ph.D.

E-mail : omsingh81@gmail.com

shodhsamagam1@gmail.com

Received on : 29/05/2026
Revised on : 30/07/2026
Accepted on : 08/08/2026
Overall Similarity : 10% on 31/07/2026



Plagiarism Checker X - Report

Originality Assessment

10%

Overall Similarity

Date: Jul 31, 2026 (12:59 PM)
Matches: 388 / 3824 words
Sources: 35

Remarks: Low similarity detected, consider making necessary changes if needed.

Verify Report:
Scan this QR Code



ABSTRACT

The rapid expansion of electronic commerce has fundamentally transformed the manner in which commercial transactions are negotiated and concluded. Electronic contracts (e-contracts), executed through emails, websites, mobile applications, and digital platforms, have become indispensable to modern business operations. India has responded to this transformation by enacting the Information Technology Act, 2000, which accords legal recognition to electronic records and digital signatures while complementing the principles of contract formation embodied in the Indian Contract Act, 1872. Despite these legislative developments, significant legal uncertainties persist concerning the validity of electronic consent, the reliability of electronic signatures, evidentiary standards for digital records, cross-border enforcement, cybersecurity risks, and the regulation of emerging technologies such as smart contracts and artificial intelligence.

KEY WORDS

Electronic Contracts, Information Technology Act, 2000, Electronic Signatures, Digital Signatures, Bharatiya Sakshya Adhiniyam, E-Commerce.

INTRODUCTION

The digital economy has transformed commercial transactions by replacing traditional paper-based agreements with electronically executed contracts. Consumers routinely purchase goods through online marketplaces, subscribe to digital services, execute banking transactions, and accept contractual terms through a single click or electronic authentication. These developments have significantly reduced transaction costs, accelerated commercial dealings, and expanded access to national and international markets. Consequently, electronic contracts have become a fundamental component of contemporary commercial law.

An electronic contract is not a distinct category of contract but rather a conventional contract concluded through electronic means. The essential requirements of a valid contract-offer, acceptance, lawful consideration, free consent, competency of parties, and lawful object-continue to be governed by the Indian Contract Act, 1872. The Information Technology Act, 2000 supplements these principles by conferring legal recognition upon electronic records and electronic signatures, thereby ensuring that contracts executed electronically possess the same legal validity as those concluded through traditional written instruments.

The enactment of the Information Technology Act, 2000 represented India's first comprehensive legislative response to electronic commerce. Inspired by the UNCITRAL Model Law on Electronic Commerce, 1996, the Act removed legal barriers arising from requirements of writing, signatures, and document retention. Subsequent amendments, particularly through the Information Technology (Amendment) Act, 2008, expanded the recognition of electronic signatures beyond conventional digital signatures, reflecting technological advancements and evolving commercial practices.

The emergence of artificial intelligence, blockchain technology, and smart contracts has further complicated the legal landscape. Automated contract formation through AI systems raises questions concerning contractual intent, allocation of liability, algorithmic decision-making, and consumer protection. Smart contracts executed through blockchain platforms challenge conventional doctrines relating to interpretation, modification, breach, and judicial intervention because contractual obligations may execute automatically without subsequent human participation.

Legal Framework Governing Electronic Contracts in India

The legal recognition of electronic contracts in India is founded on the combined operation of the Indian Contract Act, 1872 (ICA) and the Information Technology Act, 2000 (IT Act). While the ICA prescribes the substantive requirements for a valid contract, the IT Act confers legal recognition upon electronic records and electronic signatures, thereby removing barriers created by the traditional requirement of paper-based documentation. Together, these statutes establish the legal basis for electronic commerce and digital transactions in India.

Meaning and Nature of Electronic Contracts

An electronic contract (e-contract) is a legally enforceable agreement concluded through electronic means such as websites, e-mails, mobile applications, electronic data interchange (EDI), or other digital communication systems. The mode of communication differs from traditional contracts, but the substantive legal requirements remain unchanged. Consequently, an electronic contract is governed by the same contractual principles applicable to conventional agreements.

Electronic contracts possess several distinguishing characteristics. They are generally paperless, executed instantaneously across geographical boundaries, electronically stored, and authenticated through digital or electronic signatures. Their widespread use has substantially reduced transaction costs, increased commercial efficiency, and facilitated global trade.

The principal forms of electronic contracts include:

- **Click-wrap Agreements:** Users expressly indicate acceptance by clicking an "I Agree" or similar button before accessing a product or service. Courts generally regard such agreements as enforceable because they involve affirmative consent.
- **Browse-wrap Agreements:** Contractual terms are available through hyperlinks on a website, and acceptance is inferred from continued use of the website. Their enforceability depends upon whether adequate notice of the terms was provided.
- **Shrink-wrap Agreements:** Commonly used for software products, these agreements provide contractual terms inside or on product packaging, with acceptance occurring upon opening the package or installing the software.
- **E-mail Contracts:** Offer and acceptance are exchanged through electronic mail, creating legally enforceable contractual obligations when the essential requirements of contract formation are satisfied.

Although these contractual forms differ procedurally, their legal validity depends upon compliance with statutory requirements under the Indian Contract Act and the Information Technology Act.

Validity of Electronic Contracts under the Indian Contract Act, 1872

The Indian Contract Act, 1872 does not distinguish between physical and electronic contracts. Instead, it establishes universal principles applicable irrespective of the medium through which contractual consent is communicated.

Section 2(a): Proposal

Section 2(a) defines a proposal as the expression of willingness by one person to do or abstain from doing something with a view to obtaining the assent of another.

In electronic commerce, proposals frequently arise through online advertisements, electronic catalogues, price quotations, auction platforms, and commercial websites. Depending upon the circumstances, such online displays may constitute either invitations to offer or legally binding offers.

Section 2(b): Acceptance

Section 2(b) provides that a proposal becomes a promise when accepted by the person to whom it is made.

Electronic acceptance may occur through:

- Clicking an acceptance button;
- Sending an acceptance e-mail;
- Applying an electronic signature;
- Completing an online payment process; or
- Performing conduct that clearly signifies assent.

The acceptance must remain absolute and unqualified, as required by Section 7 of the Act.

Section 2(h): Contract

Section 2(h) defines a contract as an agreement enforceable by law.

Accordingly, once an electronic agreement satisfies the statutory essentials prescribed under the Contract Act, it enjoys the same legal status as a conventional written agreement.

Section 10: Essentials of a Valid Contract

Section 10 provides that agreements become contracts when made by the free consent of competent parties, for lawful consideration and lawful object, and are not expressly declared void.

Electronic contracts must therefore satisfy the following essential elements:

- Valid offer;
- Valid acceptance;
- Free consent;
- Competency of parties;
- Lawful consideration;
- Lawful object; and
- Intention to create legal relations.

The mere electronic mode of execution does not affect contractual validity.

Free Consent in Electronic Contracts

Determining free consent presents particular challenges in electronic contracting. Standard-form agreements often contain lengthy contractual clauses that consumers rarely read before clicking "I Agree." Issues relating to unequal bargaining power, unfair contractual terms, fraud, misrepresentation, and coercive digital practices have therefore become increasingly significant in online transactions.

Consequently, courts examine whether users received adequate notice of contractual terms and whether meaningful consent was obtained.

Information Technology Act, 2000

The Information Technology Act, 2000 provides the statutory foundation for electronic commerce by granting legal recognition to electronic records and electronic authentication methods. The Act substantially follows the principles embodied in the UNCITRAL Model Law on Electronic Commerce, 1996.

Section 4: Legal Recognition of Electronic Records

Section 4 provides that where any law requires information to be in writing, printed, or typewritten, such requirement shall be deemed satisfied if the information is rendered or made available in an electronic form that is accessible for future reference.

This provision eliminates the legal preference for paper documents and enables electronic records to possess equivalent legal status.

Section 5: Legal Recognition of Electronic Signatures

Section 5 recognises electronic signatures for documents requiring authentication.

Accordingly, contracts cannot be denied legal validity solely because they are authenticated electronically rather than through handwritten signatures.

This provision significantly enhances commercial certainty in electronic transactions.

Section 10A: Validity of Contracts Formed through Electronic Means

Inserted by the Information Technology (Amendment) Act, 2008, Section 10A expressly provides that contracts shall not be deemed unenforceable merely because proposals, acceptances, revocations, or communications are communicated electronically.

Section 10A represents one of the most significant provisions governing electronic commerce in India because it conclusively establishes the enforceability of electronically concluded contracts.

Sections 3 and 3A: Digital Signatures and Electronic Signatures

Section 3 recognises authentication through digital signatures based upon asymmetric cryptographic systems and hash functions.

Section 3A broadens the concept by recognising electronic signatures employing reliable electronic authentication techniques prescribed by the Central Government.

The transition from digital signatures to broader electronic signatures reflects India's adoption of technology-neutral legislative principles.

Secure Electronic Records and Secure Electronic Signatures

The IT Act further recognises secure electronic records and secure electronic signatures where prescribed security procedures ensure authenticity and integrity.

Such statutory presumptions simplify evidentiary proof during judicial proceedings and enhance confidence in electronic transactions.

Types of Electronic Signatures in India

India presently recognises multiple methods of electronic authentication.

- **Digital Signature Certificates (DSCs):** These rely upon Public Key Infrastructure (PKI), cryptographic encryption, and certificates issued by licensed Certifying Authorities under the IT Act.
- **Aadhaar-based eSign:** The eSign framework enables users to authenticate documents electronically through Aadhaar-based identity verification while maintaining statutory compliance.
- **Other Electronic Authentication Techniques:** Section 3A empowers the Central Government to notify additional reliable electronic authentication methods in response to technological developments.

This flexible statutory approach ensures that the legal framework remains technologically adaptable.

Validity and Enforceability of Electronic Contracts

Electronic contracts become legally enforceable when statutory contractual requirements coexist with valid electronic authentication under the Information Technology Act.

Important considerations include:

- Identification of contracting parties;
- Reliable authentication mechanisms;
- Attribution of electronic communications;
- Maintenance of record integrity;
- Evidence of informed consent; and
- Compliance with statutory formalities.

The IT Act therefore supplements rather than replaces the Indian Contract Act.

Nevertheless, certain documents continue to require traditional execution.

Documents Excluded from Electronic Execution

The First Schedule to the Information Technology Act excludes certain categories of documents from electronic recognition, including:

- Negotiable instruments (other than cheques);
- Powers of attorney;
- Trust deeds;
- Wills and testamentary dispositions; and
- Contracts relating to the sale or conveyance of immovable property where excluded by applicable law.

These exclusions reflect legislative concerns regarding authenticity, fraud prevention, and public registration requirements.

Evidentiary Framework for Electronic Contracts in India

The enforceability of an electronic contract depends not only on its valid formation but also on the ability of a party to prove its existence, authenticity, and integrity before a court of law. With commercial transactions increasingly conducted through e-mails, electronic platforms, mobile applications, cloud storage, and blockchain-based systems, electronic evidence has become central to modern civil and commercial litigation.

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) replaced the Indian Evidence Act, 1872 while substantially retaining the legal recognition accorded to electronic records. The BSA expressly recognises electronic and digital records as documentary evidence and seeks to accommodate technological developments in judicial proceedings. Consequently, electronic contracts authenticated through legally recognised methods enjoy the same evidentiary value as conventional written agreements, provided statutory requirements concerning authenticity and reliability are satisfied.

Electronic Signatures as Evidence

Electronic signatures perform two fundamental legal functions. First, they authenticate the identity of the contracting party. Secondly, they establish that the contents of the electronic record have not been altered after execution.

Digital Signature Certificates (DSCs), based upon Public Key Infrastructure (PKI), provide a comparatively higher degree of evidentiary reliability because they utilise cryptographic techniques capable of detecting unauthorised alterations. Similarly, Aadhaar-based eSign services facilitate secure authentication by combining identity verification with digital execution.

Despite these technological safeguards, disputes continue to arise regarding forged signatures, compromised credentials, unauthorised access, and fraudulent electronic transactions. Courts therefore examine surrounding

circumstances, including transaction history, electronic communications, system logs, IP addresses, and expert evidence, before determining the authenticity of an electronic signature.

The effectiveness of India's electronic contracting regime thus depends not merely upon statutory recognition but also upon the technological robustness of authentication mechanisms.

Judicial Analysis

Indian courts have progressively adapted traditional contractual principles to the realities of digital commerce. Judicial decisions demonstrate a consistent willingness to recognise electronically concluded agreements while simultaneously insisting upon procedural safeguards relating to electronic evidence.

Trimex International FZE Ltd. v. Vedanta Aluminium Ltd. (2010) 3 SCC 1

- **Facts:** The dispute arose from negotiations conducted primarily through electronic mail concerning the international sale of bauxite. One party subsequently refused to perform the agreement, contending that no formally executed written contract existed.
- **Issue:** Whether an exchange of e-mails could constitute a legally enforceable contract.
- **Judgment:** The Supreme Court held that a binding contract may arise through electronic communications where offer, acceptance, consideration, and intention to create legal relations are established.
- **Ratio Decidendi:** The Court emphasised that the absence of a formally signed document does not invalidate a contract if consensus ad idem is evident from electronic correspondence.
- **Significance:** The decision firmly established that electronic communications are capable of creating enforceable contractual obligations under Indian law and remains one of the leading authorities on electronic contract formation.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1

A three-judge Bench of the Supreme Court clarified the legal position regarding electronic evidence and reaffirmed that statutory requirements governing admissibility must ordinarily be satisfied. The Court overruled inconsistent interpretations emerging from earlier decisions and strengthened procedural certainty concerning electronic records.

The judgment significantly enhances the reliability of electronic contracts by ensuring that digital evidence admitted before courts satisfies established evidentiary standards.

Comparative Perspectives

United States

The United States regulates electronic contracts primarily through the Electronic Signatures in Global and National Commerce Act (E-SIGN Act), 2000 and the Uniform Electronic Transactions Act (UETA).

These statutes provide that electronic signatures and electronic records cannot be denied legal effect solely because they are electronic. The American approach is characterised by strong technological neutrality, permitting parties to utilise any reliable authentication method without prescribing a single technological standard.

This flexibility has facilitated innovation while maintaining commercial certainty.

United Kingdom

The United Kingdom recognises electronic contracts through the Electronic Communications Act 2000, common law principles, and post-Brexit retained legislation.

English courts generally focus upon the intention of the parties rather than the technological method employed for contract formation. Consequently, electronic agreements, e-mails, and electronically authenticated documents are routinely enforced provided traditional contractual requirements are satisfied.

European Union

The European Union has established one of the world's most sophisticated regulatory systems through the eIDAS Regulation (Regulation (EU) No. 910/2014).

The Regulation creates a harmonised legal framework governing electronic identification, trust services, and electronic signatures throughout Member States. It classifies electronic signatures into different categories based upon their security and reliability while facilitating cross-border recognition within the European Union.

Singapore

Singapore's Electronic Transactions Act closely follows the UNCITRAL Model Law and adopts a technologically neutral approach.

The legislation encourages electronic commerce by recognising electronic records, electronic signatures, automated transactions, and secure electronic authentication. Singapore's emphasis upon technological innovation has made it a regional leader in digital commerce regulation.

Australia

Australia regulates electronic transactions through the Electronic Transactions Act 1999, which provides legal recognition to electronic communications while adopting the principles of functional equivalence and technological neutrality.

The Australian framework permits parties considerable flexibility regarding electronic authentication while ensuring adequate protection against fraud and misuse.

Comparative Evaluation

A comparison of these jurisdictions reveals several important observations.

First, all jurisdictions recognise that electronic contracts should possess the same legal validity as conventional agreements. The principle of functional equivalence has therefore achieved widespread international acceptance.

Secondly, advanced jurisdictions increasingly adopt technologically neutral legislation rather than prescribing specific authentication technologies. Such flexibility enables legal systems to accommodate future technological developments without frequent statutory amendments.

Thirdly, regulatory emphasis has gradually shifted beyond mere recognition of electronic contracts toward cybersecurity, digital identity verification, consumer protection, privacy regulation, and cross-border interoperability.

India has successfully established the legal validity of electronic contracts through the Information Technology Act, 2000. Nevertheless, compared with jurisdictions such as the European Union and Singapore, India's regulatory framework remains comparatively fragmented in relation to digital identity governance, international recognition of electronic signatures, blockchain-based transactions, and artificial intelligence-assisted contracting.

Emerging Legal Challenges

Artificial Intelligence and Automated Contract Formation

Artificial intelligence has fundamentally transformed commercial contracting. Digital platforms increasingly employ AI systems capable of negotiating prices, recommending contractual terms, processing customer requests, and generating contractual documents without continuous human intervention.

Existing Indian contract law assumes that contractual consent originates from natural or juristic persons. The increasing autonomy of AI systems therefore challenges traditional concepts of offer, acceptance, intention, and consent. Present legislation provides little direct guidance regarding these issues.

Smart Contracts and Blockchain Technology

Smart contracts are self-executing agreements recorded on blockchain networks in which contractual obligations automatically execute once predetermined conditions are fulfilled.

These contracts offer several advantages:

- Automation of contractual performance.
- Reduced transaction costs.
- Greater transparency.
- Increased security through decentralised verification.
- Reduced dependence upon intermediaries.

However, smart contracts also generate novel legal issues.

Once deployed, blockchain transactions are generally irreversible. Consequently, traditional contractual remedies such as rescission, rectification, or modification become considerably more difficult to implement. Questions also arise regarding jurisdiction, governing law, coding errors, software vulnerabilities, and allocation of liability among developers, users, and platform operators.

India presently lacks comprehensive statutory provisions specifically regulating blockchain-based contracts.

Consumer Protection

Electronic commerce has significantly altered the balance of bargaining power between businesses and consumers.

Online contracts frequently consist of lengthy standard-form agreements drafted exclusively by service providers. Consumers often accept these agreements without reading or understanding their legal consequences.

Potential concerns include:

- Unfair contractual clauses.
- Excessive limitation of liability.
- Automatic renewal provisions.
- Mandatory arbitration clauses.
- Unilateral modification of contractual terms.
- Collection and commercial exploitation of personal data.

Although the Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020 provide important safeguards, continuous regulatory adaptation remains necessary.

Data Protection and Privacy

Electronic contracts routinely involve the collection and processing of personal information.

Businesses commonly obtain:

- Identity details.
- Financial information.
- Biometric data.
- Location information.
- Purchasing behaviour.
- Browsing history.

The enactment of the Digital Personal Data Protection Act, 2023 represents a major advancement in protecting personal data during electronic transactions. Nevertheless, effective implementation, regulatory coordination, and cross-border data governance continue to present significant legal challenges.

Cybersecurity Risks

Cybersecurity has become one of the greatest threats to electronic commerce.

Common risks include:

- Identity theft.
- Data breaches.
- Malware attacks.
- Ransomware.
- Phishing.
- Electronic signature forgery.
- Cloud security failures.

Even where an electronic contract is legally valid, cybersecurity failures may compromise its authenticity and evidentiary reliability.

Consequently, technical safeguards are becoming as important as legal safeguards.

Recommendations

Based upon the foregoing analysis, the following reforms are recommended.

Legislative Reforms

- Amend the Information Technology Act, 2000 to expressly regulate artificial intelligence-assisted contracts and blockchain-based smart contracts.
- Introduce statutory provisions governing automated decision-making in contractual relationships.
- Periodically review excluded categories of documents in light of technological developments.

Judicial Reforms

- Develop specialised judicial training programmes concerning electronic evidence, blockchain technology, artificial intelligence, and cybersecurity.
- Encourage uniform judicial standards regarding authentication of electronic records.

Regulatory Reforms

- Establish comprehensive standards governing electronic identity verification.
- Promote interoperability between Indian electronic signature systems and internationally recognised authentication frameworks.
- Strengthen regulatory coordination between digital commerce, cybersecurity, and data protection authorities.

CONCLUSION

The emergence of electronic contracts has fundamentally transformed commercial transactions by replacing conventional paper-based agreements with technologically enabled contractual relationships. As businesses, financial institutions, Government agencies, and consumers increasingly rely on digital platforms, the legal system must ensure that electronic contracts remain reliable, enforceable, and capable of protecting the legitimate interests of all contracting parties. India's legal framework, primarily comprising the Indian Contract Act, 1872 and the Information Technology Act, 2000, has largely succeeded in providing statutory recognition to electronic contracts by removing legal barriers associated with electronic records and electronic signatures.

The analysis undertaken in this paper demonstrates that electronic contracts are not a separate category of contracts but are governed by the same foundational principles applicable to traditional agreements. The essential requirements of offer, acceptance, lawful consideration, free consent, competency of parties, and lawful object continue to determine contractual validity irrespective of whether the agreement is concluded physically or electronically. The Information Technology Act, 2000 complements these principles by recognising electronic records, digital signatures, and electronic signatures, while **Section 10A** expressly validates contracts formed through electronic means.

Judicial decisions have further strengthened the enforceability of electronic contracts. The Supreme Court in *Trimex International FZE Ltd. v. Vedanta Aluminium Ltd.* affirmed that an exchange of e-mails may constitute a binding contract where the essential elements of contract formation are established. Likewise, decisions concerning electronic evidence, particularly *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, have reinforced the procedural safeguards governing the admissibility and reliability of electronic records. These developments collectively demonstrate the judiciary's willingness to adapt established legal principles to the realities of digital commerce.

Despite these achievements, several challenges remain unresolved. The Information Technology Act, 2000 was enacted when electronic commerce was still in its formative stage. Contemporary technologies-including artificial intelligence, blockchain-based smart contracts, cloud computing, biometric authentication, and decentralised digital platforms-have significantly altered the nature of contractual relationships. Existing legislation provides only limited guidance regarding AI-generated contracts, automated contractual performance, allocation of liability for algorithmic decisions, and blockchain-enabled transactions.

BIBLIOGRAPHY

1. Agarwala, K. (2017) *Business on the Net: An Introduction to the Electronic Commerce*. Macmillan India, New Delhi.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
3. Avtar, S. (2022) *Law of Contract and Specific Relief* (13th ed.) Eastern Book Company, Lucknow.
4. Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India)
5. Consumer Protection (E-Commerce) Rules, 2020.
6. Consumer Protection Act, No. 35 of 2019 (India)
7. Digital Personal Data Protection Act, No. 22 of 2023 (India)
8. Electronic Communications Act 2000 (UK)
9. Electronic Transactions Act 1999 (Cth) (Australia)
10. Electronic Transactions Act 2010 (Singapore)
11. EUR-Lex. <https://eur-lex.europa.eu>, Accessed on 02/04/2026.
12. India Code. <https://www.indiacode.nic.in>, Accessed on 07/02/2026.
13. Indian Contract Act, No. 9 of 1872 (India)
14. Information Technology Act, No. 21 of 2000 (India)
15. Law Commission of India. (2003) *180th Report on Article 20(3) of the Constitution of India and the Right to Silence*. Government of India, New Delhi.
16. Ministry of Electronics and Information Technology. (2023) *Information Technology Act, 2000*. <https://www.meity.gov.in>, Accessed on 17/03/2026.
17. Ministry of Electronics and Information Technology. <https://www.meity.gov.in>, Accessed on 08/05/2026.
18. Mulla, D. F. (2021) *Mulla on the Indian Contract Act* (16th ed.) LexisNexis, Gurgaon.
19. National Informatics Centre. (2024) *Digital Signature Services in India*. <https://www.nic.in>, Accessed on 08/12/2025.
20. Pollock, F. & Mulla, D. F. (2019) *The Indian Contract Act and Specific Relief Acts* (16th ed.) LexisNexis, Gurgaon.
21. Rattan, J. K. (2021) *Cyber Laws and Information Technology*. Bharat Law House, New Delhi
22. Reed, C. (2004) Electronic contracts: To what extent has the paperless office arrived? *Computer Law & Security Review*, 20(5), 346–352.
23. Singh, T. (2022) *Information Technology Law and Practice*. Universal Law Publishing, New Delhi.
24. Sneddon, A. (2011) Legally binding click-wrap agreements. *International Journal of Law and Information Technology*, 19(3), 269–293.
25. Trimex International FZE Ltd. v. Vedanta Aluminium Ltd., (2010) 3 SCC 1.
26. UNCITRAL. <https://uncitral.un.org>, Accessed on 17/03/2026.
27. United Nations Commission on International Trade Law. (1996) *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*. United Nations, New York.
28. United Nations Commission on International Trade Law. (2001) *UNCITRAL Model Law on Electronic Signatures*. United Nations, New York.
29. United Nations Convention on the Use of Electronic Communications in International Contracts, 2005.
30. Winn, J. K. (2002) The Emperor's New Clothes: The Shocking Truth About Electronic Commerce Law. *Berkeley Technology Law Journal*, 17(1), 213–258.
