Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

From Paper to Pixels: Evolution of Contract Formation in the Era of Electronic Contracts

Shriram Jadhav[a] Ved Shimpi[b]

[a]Maharashtra National Law University, Mumbai, India [b]Maharashtra National Law University, Mumbai, India

Received 15 April 2026; *Accepted* 19 May 2026; *Published* 23 May 2026

The digitalisation of commerce has significantly transformed the manner in which contracts are negotiated, executed, and enforced in India. This article examines the changing landscape of Indian e-contract jurisprudence and the legal challenges emerging from electronic transactions. It analyses the interaction between the Indian Contract Act, 1872, the Information Technology Act, 2000, and the Indian Evidence Act, 1872, in providing legal validity to digital agreements and electronic evidence. Through landmark decisions such as the State of Punjab & Ors. v Amritsar Beverages Ltd., Anvar P.V. v P.K. Basheer, South West Terminal Ltd. v Achter Land & Cattle Ltd., and Trimex International FZE Ltd. v Vedanta Aluminium Ltd., the article explores important developments concerning electronic signatures, admissibility of digital records, and non-traditional forms of consent such as emojis. It further highlights concerns relating to authentication, cyber fraud, Section 65B compliance, and AI-generated contracts. The study concludes that although Indian courts have adopted a technologically adaptive and pragmatic approach, comprehensive legislative reforms are necessary to strengthen the future of digital contracting in India.

Keywords: *e-contract, digital, admissibility, validity, e-signature.*

INTRODUCTION

The promise of contract law has always been simple: voluntary agreements between competent parties shall be recognised and enforced by the state. For over a century and a half, Indian contract jurisprudence discharged this promise through the medium of paper, ink, and physical presence. The Indian Contract Act 1872[1], drafted in an era of telegrams and trade by correspondence, was deliberately indifferent to medium, describing the conditions of a valid contract without mandating any particular form. This medium-neutrality proved to be the Act's greatest virtue as the digital revolution arrived without seeking the law's permission.

By the turn of the twenty-first century, commerce was being conducted through websites, email threads, and electronically transmitted instruments at a velocity that paper-based contracting could not sustain. Parliament's response was Section 10A of the Information Technology Act, 2000,[2] which extended unambiguous statutory recognition to contracts formed through electronic means. The provision was modest in its drafting; its consequences were profound. In the decades since, Indian courts have been required to answer questions of mounting complexity: Are electronic records admissible as documentary evidence? Can a digital signature be repudiated on identity grounds? Does an emoji constitute binding acceptance? Must click-wrap consent satisfy data protection standards?

This article maps the developing jurisprudence across five key developments, examining one landmark decision for each. The objective is not merely to chronicle change but to identify the doctrinal principles crystallising beneath the surface of these decisions, and to assess their adequacy for the demands of contemporary digital commerce.

STATUTORY FRAMEWORK

Three legislative instruments provide the primary architecture of Indian e-contract law. The Indian Contract Act, 1872 establishes the substantive conditions of contractual validity, competence, lawful object, free consent, and consideration in terms that are entirely medium-neutral.[3] Section 10A of the IT Act, 2000 supplies the digital validation layer, affirming that

[1] Indian Contract Act 1872, s 1
[2] Information Technology Act 2000, s 10A
[3] Indian Contract Act 1872, s 10

no contract shall be denied legal effect solely because it was formed electronically. The Indian Evidence Act, 1872, particularly Section 65B as amended in 2000,[4] governs the admissibility of electronic records in legal proceedings, a provision that has generated its own substantial body of case law.

Two further instruments have assumed increasing relevance. The Digital Personal Data Protection Act, 2023 (DPDPA)[5] has introduced a high-standard consent framework for data processing, with direct implications for the design of digital contracts. The Controller of Certifying Authorities under the IT Act administers the regime for digital signature certificates, providing the public-key infrastructure on which legally secure digital execution depends.[6] Certain transactions remain outside the scope of digital execution: negotiable instruments, powers of attorney requiring registration, wills, and instruments creating or transferring immovable property rights cannot be validly executed electronically.

FIVE KEY DEVELOPMENTS: CASE LAW ANALYSIS

Development 1: Judicial Recognition of Electronic Records as Evidence: The admissibility of electronic records in Indian legal proceedings is governed by Sections 65A and 65B of the Indian Evidence Act, 1872, inserted by the IT Act, 2000. Section 65B requires that a certificate be furnished by a responsible official of the computer system from which the record was generated, attesting to the system's regular operation and the record's integrity.[7] For over a decade, courts disagreed on whether this certificate was a condition precedent to admissibility or merely a procedural rule that could be waived.

The Supreme Court's landmark ruling in the State of Punjab & Ors. v Amritsar Beverages Ltd.[8], the dispute arose when the State of Punjab relied on computer-generated tax and commercial records of Amritsar Beverages Ltd. to establish liability under excise laws. The company challenged the admissibility of these electronic records, arguing that they did not comply with the requirements of Section 65B of the Indian Evidence Act, 1872[9]. The case reached the Supreme Court to determine whether such electronically generated records,

[4] Indian Evidence Act 1872, ss 65A–65B
[5] Digital Personal Data Protection Act 2023, ss 6–7
[6] Information Technology Act 2000, ss 17–34
[7] Indian Evidence Act 1872, s 65B(4); Pavan Duggal, *Cyberlaw: The Indian Perspective* (2nd edn, Saakshar Law Publications 2016) 211–30
[8] *State of Punjab and Ors v M/S Amritsar Beverages Ltd and Ors* (2006) 7 SCC 607
[9] Indian Evidence Act 1872, s 65B

produced in the ordinary course of business, could be accepted as valid evidence and under what conditions. It directly addressed the evidentiary threshold for electronically generated tax and commercial records, affirming that electronic documents produced from computers operating in the ordinary course of business are admissible when accompanied by the requisite statutory certificate and adequate proof of system reliability.

Held: Electronic records generated from computer systems operating in the ordinary course of business are admissible as evidence under Section 65B of the Indian Evidence Act, 1872, provided the conditions specified in the provision are substantially satisfied. The Court affirmed that the certificate requirement under Section 65B(4) serves a non-waivable authenticity function.

The significance of this ruling for digital contracting is foundational. Any party intending to rely on an electronic agreement, email acceptance, or digitally executed instrument in adversarial proceedings must secure a Section 65B certificate from the system administrator of the relevant platform at the time of document execution, not merely at the time of litigation.[10] Academic commentary has noted that this rigidity creates evidentiary barriers that disproportionately burden individuals and smaller entities without dedicated IT governance infrastructure.[11] The decision must be read alongside the Supreme Court's subsequent, authoritative resolution of the Section 65B controversy in Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020),[12] which conclusively confirmed the mandatory nature of the certificate as a condition precedent to admissibility.

Development 2: E-Signature Validity and Identity Authentication Disputes: Electronic signatures have proliferated across Indian commerce in loan disbursements, employment agreements, lease contracts, and consumer financial products. The IT Act distinguishes between 'electronic signatures' (a broader category encompassing OTP authentication and biometric verification) and 'digital signatures' (a narrower category requiring a certificate from a licensed Certifying Authority, carrying a higher presumption of validity).[13] The

[10] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal and Ors* AIR 2020 SC 4908
[11] Nandan Kamath, *Law Relating to Computers Internet and E-commerce: A Guide to Cyberlaws and the Information Technology Act, 2000 with Rules, Regulations and Notifications* (3rd edn, Universal Law Publishing 2017) 312–25
[12] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal and Ors* AIR 2020 SC 4908
[13] Information Technology Act 2000, ss 2(ta), 3 and 3A; Information Technology (Certifying Authority) Regulations 2001, sch I

practical consequence is a two-tier authentication ecosystem in which courts have been required to adjudicate disputes about attribution and consent.

In Anvar P.V. v P.K. Basheer[14], the dispute arose from an election petition where the admissibility of electronic evidence (such as digital recordings) was questioned. The party sought to rely on electronic records without complying with the procedural requirements under Section 65B of the Indian Evidence Act, 1872. The Supreme Court was called upon to determine whether such electronic evidence could be admitted without proper certification, ultimately laying down the governing framework for the admissibility of all electronic records in Indian legal proceedings. Supreme Court decision that conclusively resolved the admissibility framework for electronic records in the context of a disputed election petition and, by necessary extension, for all digital evidence in Indian legal proceedings.

Held: Electronic records are a distinct category of evidence; oral evidence of the contents of an electronic record is not permissible. Admissibility requires full compliance with the requirements of Section 65B of the Indian Evidence Act, 1872. The Court clarified that electronic records stand outside the conventional framework of primary and secondary evidence and constitute their own evidentiary category.

The analysis from Anvar P.V. is directly applicable to e-signature disputes: a party cannot simply testify to the contents or execution of a digital agreement. The digital record itself, properly certified, must be produced. This reinforces the importance of platform-level record retention policies in digital contracting ecosystems.[15] The decision's framework, subsequently reinforced in Arjun Panditrao Khotkar (2020),[16] means that courts examining contested e-signatures must scrutinise the complete authentication chain: who initiated the request, what credentials were verified, through which device, and whether any anomalies in the process are explicable consistently with genuine consent.

Development 3: Non-Traditional Digital Consent: The Emoji Contract Debate: The transformation of commercial communication onto instant messaging platforms WhatsApp, Telegram, and similar services has produced a novel legal question: can informal digital symbols, including emojis, constitute legally cognisable acceptance of a contractual offer?

[14] *Anvar PV v PK Basheer and Ors* (2014) 10 SCC 473
[15] *Shafhi Mohammad v State of Himachal Pradesh* (2018) 5 SCC 311
[16] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal and Ors* AIR 2020 SC 4908

Under classical Indian contract law, acceptance must be absolute and unequivocal (Section 7, Indian Contract Act) and must be communicated in the form prescribed or reasonably implied by the offeror (Section 4).[17] The question is whether a digital symbol, such as a thumbs-up emoji, satisfies these requirements in the context of a commercial transaction.

The landmark authority on this question is the Canadian decision, South West Terminal Ltd. v Achter Land and Cattle Ltd., 2023 (Court of King's Bench, Saskatchewan)[18], which has attracted serious attention in Indian legal commentary for its direct relevance to Section 7 of the Indian Contract Act[19]. The dispute arose between two commercial parties engaged in a prior course of dealings in flax trading. The seller sent a photograph of a signed contract via text message, to which the buyer responded with a thumbs-up emoji. When the buyer later failed to perform, he argued that the emoji did not constitute acceptance. The Court of King's Bench, Saskatchewan, had to determine whether this digital response amounted to valid consent, ultimately holding that in the given commercial context, the emoji signified clear acceptance of the contract.

Held: A thumbs-up emoji sent by a buyer in response to a draft flax contract communicated via text message constituted valid acceptance of the agreement. The Court found that the emoji, in the specific commercial context between parties with an established trading relationship, unambiguously communicated assent. Judgment was entered for CAD 82,200.

The decision's logic is consistent with Indian doctrine: acceptance need not be expressed in any particular form, only unequivocally communicated. The critical analytical move in South West Terminal examines the course of dealing between the parties to determine that the understood meaning of the symbol maps precisely onto the Indian concept of consensus ad idem.[20] However, the decision cannot be applied mechanically to Indian facts; an emoji exchanged in an established commercial relationship carries a very different legal weight from one sent between strangers. Indian courts would need to examine prior dealings, commercial context, and any applicable trade usage.

[17] Indian Contract Act 1872, ss 4, 7; Avtar Singh, *Contract and Specific Relief* (12th edn, Eastern Book Company 2020) 67–89
[18] *South West Terminal Ltd v Achter Land and Cattle Ltd* [2023] SKKB 116 (Canada)
[19] Indian Contract Act 1872, s 7
[20] *Bhagwandas Goverdhandas Kedia v M/S Girdharilal Parshottamdas & Co and Ors* AIR 1966 SC 543

The emoji contract debate will intensify as digital commerce migrates further onto informal messaging platforms. India's extraordinarily high volume of WhatsApp-mediated commercial negotiation, particularly in agricultural commodity trading and SME supply chains[21] means that judicial clarity in this area carries significant practical stakes.

Development 4: Digital Signature Validity and Technological Neutrality: The enforceability of agreements executed through digital signatures has generated a distinct strand of Indian litigation, primarily in the financial services sector. The IT Act's two-tier framework, distinguishing the higher-grade 'digital signature' (Certifying Authority-issued, cryptographically secure) from the broader 'electronic signature' (including OTP and biometric verification), has not always been consistently applied by courts. Judicial clarifications have progressively reinforced the principle of technological neutrality: that the law does not prefer any particular authentication technology, only that the technology employed must be fit for purpose.

In Trimex International FZE Ltd., Dubai v Vedanta Aluminium Ltd.,[22] the dispute arose out of negotiations for the supply of bauxite, where the parties conducted their dealings through a series of emails and other electronic communications. Although a formal written contract was never executed, the correspondence reflected agreement on essential terms such as quantity, price, and delivery. When one party later refused to perform, it contended that no binding contract existed in the absence of a formally signed document. The Supreme Court was therefore called upon to determine whether an enforceable contract could arise solely from electronic communications, ultimately holding that the email exchanges, read as a whole, demonstrated a clear intention to be bound and thus constituted a valid contract. The leading Supreme Court authority for the proposition that digital contracting channels satisfy the requirements of offer and acceptance.

Held: A contract can be concluded through electronic communications, including email exchanges. The exchange of emails constituted a valid and binding contract where the essential terms were agreed upon, and the intention to be bound was evident from the

[21] *Internet in India 2023* (Internet and Mobile Association of India 2023) 28–34; *Report on Currency and Finance 2022–23* (Reserve Bank of India 2023) 145

[22] *Trimex International FZE Ltd, Dubai v Vedanta Aluminium Ltd, India* (2010) 3 SCC 1

correspondence as a whole. The Court affirmed that electronic communications are sufficient to meet the requirements of offer and acceptance under the Indian Contract Act, 1872.

Although predating the current wave of e-signature disputes, Trimex remains the foundational Indian authority establishing that digital communication channels satisfy the requirements of offer and acceptance under Sections 4 and 7 of the Indian Contract Act.[23] Its significance for authentication disputes is foundational: it establishes that courts will look to the totality of digital communications to identify contractual intention, rather than demanding any single formal act of execution.[24] Where identity is disputed, this holistic approach requires examining the full digital trail of device metadata, IP logs, OTP records, and subsequent conduct, not merely the fact of an electronic signature.

The principle of technological neutrality consistently affirmed across this jurisprudence provides a stable foundation for authentication standards that can evolve with technology without requiring constant legislative intervention. Its limitation is that neutrality without minimum standards permits authentication mechanisms of radically different quality to coexist under the same legal roof, a gap that the legislature or the Controller of Certifying Authorities should address through sector-specific authentication requirements.

EMERGING THEMES AND PERSISTENT CHALLENGES

Five thematic currents emerge from the analysis above. **First**, there is an unmistakable shift from formal to functional analysis: courts consistently look to the substance of intention rather than the form of execution. **Second**, authentication has displaced acceptance as the primary site of e-contract litigation. Third, the scope of legally cognisable consent is expanding from authenticated clicks to emoji symbols, demanding that the law develop more nuanced tools for distinguishing contractual commitment from ambient digital communication. **Fourth**, the boundaries between contract law, data protection, and constitutional rights are dissolving. **Fifth**, equity of access to the digital contracting ecosystem, the digital divide is emerging as a fundamental justice concern requiring a proactive regulatory response.

[23] Indian Contract Act 1872, ss 4, 7
[24] *M/s Shakti Bhog Foods Limited v Kola Shipping Ltd* (2009) 2 SCC 134

Four persistent challenges dominate the landscape. Identity verification in cross-border digital contracts remains technically complex and legally unsettled. The evidentiary demands of Section 65B compliance continue to create disproportionate burdens on smaller parties. Cyber fraud and misuse of digital credentials represent a systemic integrity risk that authentication standards alone cannot eliminate. And the pace of technological change with artificial intelligence beginning to generate and negotiate contracts without human intervention is creating a category of digital agreement for which current legal frameworks are entirely unprepared.

CONCLUSION

The four developments examined in this article, read together through their lead authorities, tell a coherent and encouraging story: Indian courts are building a digital contract jurisprudence that is doctrinally grounded, pragmatically flexible, and increasingly attentive to the quality, not merely the fact, of digital consent and authentication. State of Punjab v Amritsar Beverages Ltd. anchors the evidentiary regime for electronic records. Anvar P.V. v P.K. Basheer establishes the primacy of Section 65B certification. South West Terminal Ltd. v Achter Land & Cattle Ltd. opens the conversation on non-traditional digital acceptance. And Trimex International supplies the foundational endorsement of e-contract validity. Together, these decisions construct the doctrinal architecture within which all future development must take place.

The work is, however, far from complete. The gap between the sophistication of the technology transforming contract formation and the adequacy of the legal frameworks governing it remains uncomfortably large. Legislative reform, particularly on smart contract validity, minimum authentication standards, and the simplification of Section 65B compliance, is overdue. The transformation from paper to pixels is a transformation of medium, not of purpose. Contract law exists to give enforceable effect to voluntary human agreements. That purpose has not changed. What has changed profoundly and irreversibly is the technical sophistication required to discharge it faithfully in a networked world. The case law surveyed in this article demonstrates that Indian courts are rising to that challenge with doctrinal intelligence. The legislature must now match its pace.