JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

E-CONTRACTS IN INDIA: LEGAL FRAMEWORK AND EMERGING ISSUES

Dr Manveer Kaur[1] Dr Inderpreet Kaur [2]

Abstract

The rapid proliferation of e-commerce and platformized services has transformed how parties negotiate, conclude, and perform contracts in India. Electronic contracts (e-contracts) now mediate everything from consumer purchases and app subscriptions to business-to-business (B2B) supply chains and fintech services. The COVID-19 pandemic accelerated this shift, normalizing "contactless" contracting via click-wrap, browse-wrap, shrink-wrap, and e-mail agreements and embedding electronic signatures (e-sign/digital signatures) into enterprise workflows. This paper offers a doctrinal and policy analysis of India's legal regime governing e-contracts, centring on the ***Indian Contract Act, 1872****, the* ***Information Technology Act, 2000****, and the* ***Bharatiya Sakshya Adhiniyam, 2023*** *(successor to the Indian Evidence Act, 1872). It explains how classic elements offer, acceptance, consideration, intention, capacity, consent, lawful object translate into the digital context; examines the evidentiary status of electronic records; and maps the role of public policy in calibrating enforceability, especially where standard-form terms, asymmetric bargaining power, and data-intensive architectures intersect. The paper also assesses Electronic Data Interchange (EDI), automated contracting, and platform governance, and identifies gaps around cybersecurity, cross-border enforcement, privacy, and the evidentiary authentication of machine-generated records. It concludes that Indian law broadly recognizes e-contracts but would benefit from targeted reforms guidance on online assent, clearer rules for cross-border jurisdiction, stronger consent transparency, and sector-specific standards to enhance legal certainty while safeguarding consumer and societal interests.*

Keywords: Electronic Contracts; Information Technology Act; Digital Signatures; Bharatiya Sakshya Adhiniyam; Public Policy.

I. Introduction

India's contract law architecture rests on the **Indian Contract Act, 1872** ("Contract Act"), which supplies the canonical elements of enforceability: offer and acceptance, lawful consideration, intention to create legal relations, capacity, free consent, and lawful object.[1] Contracts opposed to law or *public policy* are void ab initio because their enforcement would injure the public or frustrate statutory purposes.[2] This elasticity especially in the judge-made doctrine of public policy has allowed courts to accommodate new socio-economic realities over time.

Digitization has reconfigured this landscape. Consumer markets now operate through apps and online marketplaces (e.g., retail platforms, mobility, food delivery), and enterprise supply chains increasingly rely on

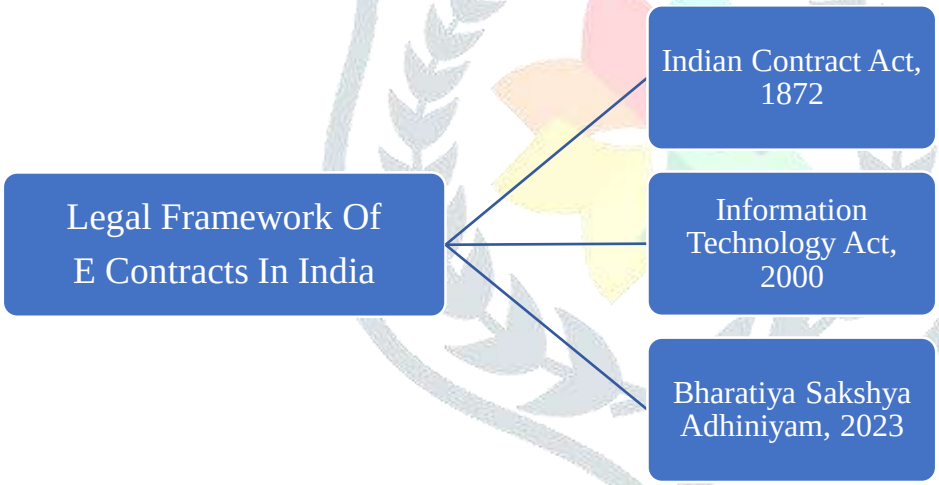
[1] Assistant Professor, Army Institute of Law, Mohali
[2] Assistant Professor, Army Institute of Law, Mohali

automated data flows (e.g., e-invoicing, EDI, API-driven procurement). The pandemic catalyzed widespread adoption of e-sign and remote workflows. These developments are underwritten by a statutory triad: (i) the Contract Act for substantive validity, (ii) the **Information Technology Act, 2000** ("IT Act") for the legal recognition of electronic records and signatures, and (iii) the **Bharatiya Sakshya Adhiniyam, 2023** ("BSA 2023") for the admissibility and authentication of electronic evidence.[3] The regime broadly aligns with international best practices such as the **UNCITRAL Model Law on Electronic Commerce (1996)**.[4]

Yet modern risks platform power, information asymmetry, dark patterns, cybersecurity incidents, and cross-border complexity raise questions about consent quality, unfair terms, and remedies. Indian courts have begun to interact with these questions through cases that recognize contract formation via electronic communications and scrutinize standard-form terms where necessary.[5] Going forward, the challenge is to preserve the efficiency gains of digital contracting while ensuring fairness, transparency, and data protection.

This paper proceeds in four steps after this Introduction: Section II delineates the statutory framework and essentials of validity; Section III examines the modalities of digital contracting (click-wrap/browse-wrap/shrink-wrap/e-mail), the mechanics of acceptance, signatures, and EDI; Section IV evaluates public policy, privacy, consumer protection, and evidentiary enforcement; Section V concludes with reform proposals.

II. Legal Framework of E-Contracts in India



A. Continuity of Classical Contract Elements

Indian law does not create a separate species called the "e-contract." Rather, it applies the Contract Act's classical elements to a digital environment. An e-contract must still display: a definite offer; unambiguous acceptance communicated to the offeror; consideration (executed or executory); intention to create legal relations (generally presumed in commerce); capacity under **Section 11**; free consent under **Section 14** (i.e., absence of coercion, undue influence, fraud, misrepresentation, mistake); and a lawful object under **Section 23**.[6]

In the digital context, these elements are often evidenced through logs, timestamps, system notices, and recorded user journeys (e.g., consent screens). The practical inquiry is whether the interface communicated the terms clearly and whether the user's conduct signalled informed assent.

B. The IT Act, 2000: Recognition of Electronic Records and Contracts

Three provisions are particularly important:

- **Section 4** accords legal recognition to *electronic records*: information that would ordinarily be in writing is not denied validity solely because it is in electronic form.[7]
- **Section 5** recognizes *digital signatures* (and by extension, notified electronic signatures) as functionally equivalent to handwritten signatures for authentication.[8]
- **Section 10A** confirms the *validity of contracts formed through electronic means*, provided the Contract Act's essentials are satisfied.[9]

These provisions neutralize form-based objections—i.e., that "no paper, no pen, no contract." In practice, Indian enterprises use (a) **digital signature certificates (DSCs)** backed by a public key infrastructure, (b) **Aadhaar-based e-sign** for certain use-cases, and (c) internal e-sign tools with audit trails for low-risk transactions.

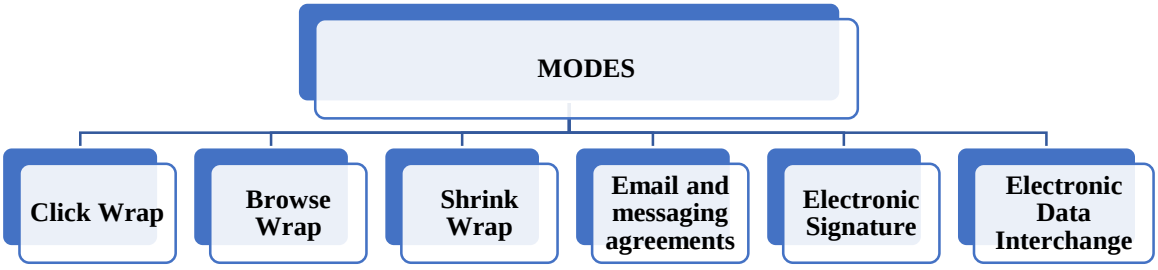
C. Bharatiya Sakshya Adhiniyam, 2023: Admissibility and Authentication

The BSA 2023 expressly recognizes *electronic records* as documentary evidence, subject to conditions ensuring integrity and authenticity (hash values, metadata, logs, certificates).[10] While its structure modernizes the Indian Evidence Act's approach, the functional goal is familiar: courts must be satisfied that an electronic record is what it purports to be and has not been tampered with. Party systems, chain-of-custody, and the reliability of secure time-stamps can be pivotal.

D. International Alignment and Soft Law

India's approach resonates with the **UNCITRAL Model Law on Electronic Commerce (1996)** and related instruments that champion *functional equivalence* (electronic functional parity with paper) and *technology neutrality*.[11] The **International Chamber of Commerce (ICC)** has long endorsed electronic contracting practices and model clauses that clarify online assent and record-keeping.[12] Such soft-law materials can guide drafting and platform governance even when not binding.

III. Modes of Digital Contracting and Mechanics of Formation



A. Click-Wrap

Click-wrap terms appear in a dialogue box or screen, requiring the user to click "I Agree" (or analogous language) after being presented with or given reasonable access to the terms. Courts typically uphold click-wrap

where: (i) the user had *adequate notice*; (ii) assent is *affirmative* (no pre-ticked boxes for core terms); and (iii) the terms are not unconscionable or contrary to statute/public policy.

In *Trimex International FZE v. Vedanta Aluminium Ltd.*, the Supreme Court accepted that a contract may be concluded through e-mail exchanges without physical signatures, crystallizing the principle that *form does not defeat substance* where consensus ad idem is evident.[13] While Trimex involved e-mails, its logic recognizing electronic communications as a medium of assent supports the enforceability of click-wrap agreements where records show informed, intentional acceptance.

Design implications. Platforms should (a) present terms conspicuously; (b) require an explicit act; (c) separate consent for key terms (e.g., arbitration, data-sharing) where appropriate; and (d) maintain robust logs tying a user identity to the consent event.

B. Browse-Wrap (Web-Wrap)

Browse-wrap presumes assent from use of a website or app without a positive click, often by placing "Terms of Use" in a footer. Enforceability turns on *notice*. If terms are obscure, courts may doubt whether a reasonable user was aware of them, especially for onerous clauses. In consumer contexts, browse-wrap is risky for core obligations (e.g., arbitration, class waivers, data-sharing). Best practice nudges platforms to hybridize: show conspicuous prompts or require a click for material terms.

C. Shrink-Wrap

Shrink-wrap contracts accompany packaged software or devices, purporting to bind users upon opening the package or installing software. Indian courts would likely ask whether the user had a *reasonable opportunity* to review terms before being bound and whether any clause is unconscionable or statutorily impermissible. For high-value or sensitive software, suppliers increasingly migrate to click-wrap or license activation flows that record affirmative assent.

D. E-Mail and Messaging Agreements

Where parties negotiate by **e-mail** or even enterprise messaging tools, a contract may arise if communications evidence agreement on essential terms and an intention to be bound. Trimex confirms that **physical signatures are not prerequisites**, though they remain good practice for clarity.[14] Parties should avoid ambiguity by drafting subject lines, recitals, and "entire agreement" language, and by consolidating the final confirmation (e.g., "Confirmed and binding subject to attached T&Cs").

E. Electronic Signatures and Authentication

Under the IT Act, **digital signatures** (using asymmetric cryptography with a certifying authority) enjoy statutory recognition.[15] The law also provides for **electronic signatures** notified by the government (e.g., Aadhaar e-Sign in approved workflows). In practice:

- **High-risk contracts** (e.g., M&A, large loans) often use DSCs and PKI with multi-factor authentication.

- **Medium-risk contracts** may use vendor e-sign solutions with secure audit trails.
- **Low-risk click-wrap** relies on server logs tied to user accounts and device identifiers.

The key is *linkage*: the system should reliably connect the individual (or corporate agent) to the act of signing or clicking, with time-stamps, IP/device data, OTP events, and tamper-evident logs.

F. Electronic Data Interchange (EDI) and Automated Contracts

EDI enables machine-to-machine exchange of structured documents—purchase orders, acknowledgments, invoices—using standardized formats. In a typical supply chain, a retailer's system dispatches an electronic purchase order; a supplier's system auto-confirms; fulfillment and invoicing follow—all without manual intervention. The legal question is whether this sequence evidences *offer* and *acceptance* by authorized agents under the Contract Act, which it generally does, provided parties have agreed to EDI protocols (often via a master supply agreement).

Advantages. Faster cycles, reduced errors, lower transaction costs, auditability, and improved cash flows.

Risks. Cybersecurity incidents, interoperability failures, and attribution disputes (who sent the message?) underscore the need for robust controls (mutual authentication, message digests, transaction IDs, non-repudiation services).

IV. Public Policy, Privacy, and Evidentiary Enforcement

A. Public Policy as a Calibrating Doctrine

Public policy under **Section 23** of the Contract Act invalidates agreements whose object or consideration is unlawful or injurious to the public.[16] The Supreme Court has emphasized that public policy is a *dynamic* concept responsive to social change.[17] In the digital setting, courts can deploy this doctrine to check exploitative standard-form clauses, penalize dark patterns that manipulate consent, and invalidate terms that contract around statutory protections (e.g., privacy rights or mandatory consumer safeguards).

Two lines of scrutiny are common:

1. **Substantive fairness**—Are terms unconscionable given information asymmetry and take-it-or-leave-it interfaces?

2. **Procedural fairness**—Did the interface provide *real* notice and a reasonable opportunity to review? Were key terms highlighted?

Where terms are egregious, courts may strike them down or read them narrowly.

B. Consumer Protection and Platform Governance

E-contracts in consumer markets often rely on boilerplate T&Cs. The **Consumer Protection Act, 2019** and e-commerce rules impose duties of transparency and prohibit unfair trade practices. Platforms should:

- Disclose key terms plainly (pricing, cancellation, data uses, dispute resolution).
- Provide accessible grievance redress.
- Avoid coercive defaults (e.g., pre-ticked boxes for add-on purchases).
- Honor statutory warranties and refund/return regimes where applicable.

Industry codes and self-regulatory mechanisms can complement statutory oversight by setting UI/UX standards for fair consent.

C. Privacy and Data Protection

E-contracts are deeply entwined with personal data—identity, payment credentials, behavioral telemetry. The **Digital Personal Data Protection Act, 2023** (DPDP Act) codifies principles of lawful processing, purpose limitation, and user rights.[18] Contracting parties that act as "data fiduciaries" must ensure transparent notices, lawful bases (consent or legitimate use), security safeguards, and breach notification where required. Contract terms that purport to waive statutory privacy rights are vulnerable under public policy and consumer law.

From a design perspective, *layered notices*, *granular consents*, and *separate prompts* for data-intensive or cross-context uses help demonstrate that consent was "free" and "informed." For B2B arrangements, **data processing addenda** should align obligations across the chain.

D. Cross-Border Enforcement and Conflict-of-Laws

Digital platforms complicate **jurisdiction** and **choice-of-law**. Best practice is to specify forum, governing law, and dispute mechanisms (e.g., institutional arbitration with seat, rules, and language). Courts examine whether such clauses are oppressive in a consumer context. For enterprise deals, **arbitration** with robust emergency relief and e-discovery protocols (including production of machine logs and source metadata) can reduce forum uncertainty.

E. Evidentiary Issues: Integrity, Attribution, and Proof

Under the BSA 2023, parties must show that an electronic record is *authentic* and *reliable*.[19] In practice, this involves:

- **Integrity evidence**: hash values, secure time-stamps, tamper-evident storage, version histories.
- **Attribution**: linking an act (click, e-sign) to a user identity via credentials, device IDs, IPs, OTP logs, or enterprise SSO.
- **System descriptions**: affidavits explaining how the platform captures and preserves records (architecture diagrams, retention policies).
- **Certificates** akin to the prior Section 65B regime, now adapted under BSA 2023 provisions, to attest to the manner and integrity of electronic production.

For **automated systems**, courts may consider whether the algorithms operated as designed and whether exceptions were flagged. Audit trails and exception reports are invaluable.

F. Risk Controls and Governance

Organizations can mitigate disputes by:

1. **Contracting Architecture**: master agreements that incorporate EDI or API terms; explicit hierarchy between T&Cs, order forms, SLAs, and privacy annexes.
2. **Consent UX**: conspicuous terms; click-through for material clauses; periodic re-consent upon material changes.
3. **Recordkeeping**: WORM (write-once-read-many) storage, cryptographic sealing, and retention schedules aligned with limitation periods.
4. **Cybersecurity**: encryption in transit/at rest, key management, least-privilege access, incident playbooks, and third-party risk assessments.

5. **Dispute Clauses**: stepped resolution (negotiation–mediation–arbitration), curated forum, and emergency measures.

V. Conclusion

Indian law has substantially embraced digital contracting. The Contract Act supplies enduring principles; the IT Act ensures functional equivalence for electronic records and signatures; the BSA 2023 modernizes evidentiary admission and authentication. Judicial developments most notably **Trimex** and long-standing doctrines around offer/acceptance and public policy confirm that **form will not trump substance** when real consensus is shown electronically. At the same time, courts remain alert to unfairness in boilerplate terms, especially in consumer contexts.

Policy priorities for the next phase include:

1. **Guidelines on Online Assent**: Government or judicial practice notes clarifying best practices for click-wrap/browse-wrap design (e.g., conspicuous presentation, separate consent for material terms, ban on dark patterns) would reduce litigation and harmonize industry behavior.

2. **Cross-Border Clarity**: Model choice-of-law and forum clauses for standardized e-commerce contexts; recognition of electronic arbitration agreements and remote hearings as default-capable.

3. **Evidentiary Tooling**: Standardized technical annexes for hash-based integrity proofs, chain-of-custody, and log schemas to streamline production under BSA 2023.

4. **Privacy by Design**: Embed DPDP Act compliance into contracting UX granular consents, data-minimization defaults, and meaningful user controls.

5. **Sectoral Standards**: In high-risk domains (fintech, health, critical infrastructure), prescribe stronger authentication, audit trails, and incident reporting around e-contract formation and performance.

6. **SME Enablement**: Toolkits and open-source templates (model T&Cs, EDI playbooks, e-sign policies) to lower compliance costs and extend digital contracting benefits beyond large enterprises.

In sum, India already recognizes the **legality, enforceability, and evidentiary admissibility** of e-contracts. The frontier is not recognition but **refinement**—making digital agreements more *understandable, fair, secure, and portable* across platforms and borders. A measured blend of legislative fine-tuning, judicial guidance, and industry self-governance can deliver a contracting ecosystem that is both innovation-ready and public-interest-centric.

References

1. *Indian Contract Act, 1872*, §§ 2(h), 10.

2. *Indian Contract Act, 1872*, § 23 (lawful object; agreements opposed to public policy void).

3. *Information Technology Act, 2000*, §§ 4, 5, 10A; *Bharatiya Sakshya Adhiniyam, 2023* (electronic evidence).

4. UNCITRAL, *Model Law on Electronic Commerce* (1996).

5. *Trimex International FZE v. Vedanta Aluminium Ltd.*, (2010) 3 SCC 1; see also general principles on standard-form contracts in *LIC v. Consumer Education & Research Centre*, (1995) 5 SCC 482.

6. *Indian Contract Act, 1872*, §§ 10–14, 23.

7. *Information Technology Act, 2000*, § 4.

8. Ibid., § 5.

9. Ibid., § 10A.

10. *Bharatiya Sakshya Adhiniyam, 2023* (electronic records; authenticity and reliability requirements).

11. UNCITRAL, *Model Law on Electronic Commerce* (1996), art. 5–8 (functional equivalence).

12. International Chamber of Commerce (ICC), guidelines and model clauses on electronic contracting (soft-law references).

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

14. Ibid.

15. *Information Technology Act, 2000*, § 5 and allied rules on digital signature certificates and certifying authorities.

16. *Indian Contract Act, 1872*, § 23.

17. *RBI v. Peerless General Finance and Investment Co. Ltd.*, (1987) 1 SCC 424 (public policy as a dynamic concept).

18. *Digital Personal Data Protection Act, 2023* (principles of lawful processing, safeguards, and data fiduciary obligations).

19. *Bharatiya Sakshya Adhiniyam, 2023* (provisions on admissibility and integrity of electronic records).

Bibliography

Primary Legislation

- *Indian Contract Act, 1872*.
- *Information Technology Act, 2000*.
- *Bharatiya Sakshya Adhiniyam, 2023*.
- *Consumer Protection Act, 2019*.
- *Digital Personal Data Protection Act, 2023*.

Cases

- *Trimex International FZE v. Vedanta Aluminium Ltd.*, (2010) 3 SCC 1.
- *Lalman Shukla v. Gauri Dutt*, (1913) ILR 35 All 489.
- *LIC v. Consumer Education & Research Centre*, (1995) 5 SCC 482.
- *RBI v. Peerless General Finance and Investment Co. Ltd.*, (1987) 1 SCC 424.

International / Soft Law

- UNCITRAL, *Model Law on Electronic Commerce* (1996).
- International Chamber of Commerce (ICC), materials on electronic contracting and model clauses.

Secondary Sources (Illustrative)

- Avtar Singh, *Law of Contract and Specific Relief* (latest ed.).
- Pollock & Mulla, *The Indian Contract Act and Specific Relief Acts* (latest ed.).
- R. Desai, "Digital Evidence and Authentication in Indian Courts," *NLSIU Law Review* (2023).
- D. Sridhar, "E-Commerce and Contract Law in India," *Journal of Cyber Law & Policy* (2022).