**End-to-end trade digitalization: Questionnaire on regulatory analysis - India**

**Introduction**

The United Nations Commission on International Trade Law (UNCITRAL) at its fifty-seventh session requested the secretariat to conduct a stocktaking exercise to examine all UNCITRAL legislative texts that referred to electronic aspects, including both UNCITRAL texts on electronic commerce and other texts that include provisions on the use of electronic means (A/79/17, para. 299). The Commission also requested a survey of the enactment of those texts and of the references to such texts contained in trade agreements. The secretariat was requested to circulate a questionnaire inviting States to provide the information and to submit copies of the relevant laws.

This Questionnaire has been prepared by the International and Comparative Law Research Center (ICLRC) as a part of its research complementing the stocktaking exercise of the secretariat and is aimed at harmonizing the existing approaches to digital trade. The main objectives of the ICLRC research are to identify the current state of implementation of the UNCITRAL documents, as well as to outline the alternative approaches and possible gaps.

This Questionnaire embraces [MLEC](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf), [MLES](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf), [ECC](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/06-57452_ebook.pdf), [MLETR](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf), [MLIT](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mlit_en.pdf), [MLAC](https://uncitral.un.org/sites/uncitral.un.org/files/mlac_en.pdf). It consolidates the UNCITRAL’s provisions on end-to-end trade digitalization based on the existing model laws and the convention in a generalized form in order to avoid duplication.

**Instructions**

This Questionnaire consists of seven parts. The first part deals with the regulatory landscape of your country. Kindly check which areas of digital trade are already covered by specific laws and briefly describe how each of the UNCITRAL General Principles is implemented in your country.

Parts II to VI are based on the relevant model laws and the convention. When answering the questions, please use one of the three colours to fill in the cells in accordance with the colour coding of the study:

|  |  |  |
| --- | --- | --- |
| **no regulation:**  the subject matter is not subject to any specific regulation in your country, but general rules of commercial or contract law may apply | **UNCITRAL regulation:**  the relevant UNCITRAL provision is fully incorporated in the laws of your country. We kindly ask you to briefly describe this regulation | **alternative regulation:** the issue addressed by the relevant UNCITRAL provision is regulated in the alternative manner by the laws of your country. We kindly ask you to briefly describe your country's approach so that we can use it for the proposals for further harmonization and consolidation of UNCITRAL instruments. |

Part VII deals with the regulatory gaps and aims at identifying the areas not yet covered by the UNCITRAL instruments.

The ICLRC would appreciate receiving responses by the end of February to allow time for compilation and analysis. The ICLRC reserves the right to make the information you provide publicly available unless you indicate otherwise.

**Part I. General**

What special laws are there in your country?

☐on electronic commerce/digital trade

|  |
| --- |
| The Information Technology (IT) Act, 2000  The Consumer Protection Act, 2019[[1]](#footnote-1): Section 94 of this Act addresses measures to prevent unfair trade practices in e-commerce and direct selling to protect consumers' interests and rights.  The Consumer Protection (E-commerce) Rules, 2020:[[2]](#footnote-2) These rules mandate transparency in product information, establish grievance redressal mechanisms, and set guidelines for e-commerce entities to ensure fair practices and enhance consumer protection. They also require e-commerce entities to display essential information, such as their name, contact details, and address, prominently on their platforms.  The Indian Contract Act, 1872:[[3]](#footnote-3) ensures that electronic contracts (e-contracts) are legally valid and enforceable, provided they meet the essential criteria of a valid contract. **The document is constantly updated. Last amendment was in 2024**[[4]](#footnote-4).  The Legal Metrology Act, 2009:[[5]](#footnote-5) This act regulates e-commerce activities, particularly concerning the standards for weights and measures of packaged goods, mandating specific labeling and packaging requirements.  Payment and Settlement Systems Act, 2007[[6]](#footnote-6): Along with the Payment and Settlement Systems Regulations, 2008, and guidelines from the Reserve Bank of India (RBI), this governs electronic payments in India.  Since 2014, the Government of India has announced various initiatives, namely Digital India[[7]](#footnote-7), Make in India[[8]](#footnote-8), Start-up India[[9]](#footnote-9), Skill India[[10]](#footnote-10), and Innovation Fund.  The Consumer Protection (e-commerce) Rules 2020 notified by the Consumer Affairs Ministry in July directed e-commerce companies to display the country of origin alongside the product listings. In addition, the companies will also have to reveal parameters that go behind determining product listings on their platforms.  Government e-Marketplace (GeM) signed a Memorandum of Understanding (MoU) with Union Bank of India to facilitate a cashless, paperless, and transparent payment system for an array of services in October 2019.  Under the Digital India movement, the Government launched various initiatives like Umang, Start-up India Portal, Bharat Interface for Money (BHIM) etc. to boost digitisation.[[11]](#footnote-11)  In October 2020, amending the equalisation levy rules of 2016, the government mandated foreign companies operating e-commerce platforms in India to have Permanent Account Numbers (PAN). |

☐on electronic/digital signatures

|  |
| --- |
| Information Technology Act, 2000 (ITA)[[12]](#footnote-12)  Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 (ESEATPR)[[13]](#footnote-13)  The Information Technology ACT (Amendments), 2008[[14]](#footnote-14)  [[15]](#footnote-15) |

☐on identity and trust services

|  |
| --- |
| Digital Personal Data Protection (DPDP) Act, 2023. It is India’s first-ever law that establishes a comprehensive legal framework for managing and safeguarding digital personal data.[[16]](#footnote-16)  The Information Technology Act, 2000[[17]](#footnote-17)  the Information Technology (Amendment) Act, 2008[[18]](#footnote-18)  Personal Data Protection Bill, 2019[[19]](#footnote-19)  National Cyber Security Policy -2013[[20]](#footnote-20) |

☐on automated contracting

|  |
| --- |
| The Indian Contract Act 1872  Information Technology Act, 2000 (ITA)[[21]](#footnote-21)  The Information Technology (Certifying Authorities) Rules 2000[[22]](#footnote-22)  Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 (ESEATPR)  The Information Technology (Use of Electronic Records and Digital Signature) Rules 2004 |

☐on electronic/digital transferrable records

|  |
| --- |
| Information Technology Act, 2000 (ITA)[[23]](#footnote-23)  THE NEGOTIABLE INSTRUMENTS ACT, 1881 |

**Adherence to the UNCITRAL General Principles**

|  |  |  |
| --- | --- | --- |
| UNCITRAL principle | Content of provision | Implementation in your country |
| Non-discrimination | Non-discrimination between information on a paper medium and information communicated or stored electronically. | Information Technology Act, 2000 deals with “validity of contracts formed through electronic means” |
| Technology neutrality | No discrimination should be made among the various techniques that may be used to communicate or store information electronically. | In 2016, the Telecom Regulatory Authority of India (TRAI) prohibited discriminatory pricing of data services, effectively banning initiatives like Facebook's Free Basics.  In 2018, the Department of Telecommunications approved TRAI's recommendations favoring net neutrality, preventing ISPs from discriminatory treatment of content, including blocking or throttling specific websites.[[24]](#footnote-24) |
| Functional equivalence | Analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques. | Information Technology Act, 2000 provides the legal framework for recognizing electronic records and digital signatures  UNCITRAL Model Laws: India's adoption of the UNCITRAL Model Law on Electronic Commerce, 1996, and the UNCITRAL Model Law on Electronic Signatures, 2001, through amendments to the IT Act.[[25]](#footnote-25) |

Part II. Electronic communications

no regulation, UNCITRAL regulation, alternative regulation

|  |  |  |
| --- | --- | --- |
| UNCITRAL provision | Content of provision | Implementation in your country |
| Consent to use | Nothing requires a party to use or accept electronic communications, but a party’s agreement to do so may be inferred from the party’s conduct. | No regulation  The Information Technology Act, 2000, but it does not explicitly mandate that parties must use or accept electronic communications; rather, it offers a legal framework for those who choose to engage in electronic transactions.  For certain types of communications explicit consent may be required under The Digital Personal Data Protection Act, 2023 (DPDP Act) |
| Technological neutrality of communication | The rules do not depend on or presuppose the use of particular types of technology and could be applied to communication and storage of all types of information. | The Information Technology Act, 2000 (IT Act) (section 2) exemplifies this principle by providing legal recognition to electronic records and digital signatures without prescribing the use of particular technologies.  The Telecom Regulatory Authority of India – rules supporting net neutrality, prohibiting any form of data discrimination by internet service providers. |
| Writing | The requirement to be in writing is met if the information is accessible so as to be usable for subsequent reference. | Under the Information Technology Act, 2000 (IT Act) (section 4) of India, the legal requirement for information to be "in writing" is satisfied if the information is:   * rendered or made available in an electronic form; and * accessible so as to be usable for subsequent reference. |
| Original | Requirement to be in original is met if the integrity of the information is assured from the time when it was first generated in its final form and, where it is required that the information it contains be made available, that information is capable of being displayed to the person to whom it is to be made available. | Under the Information Technology Act, 2000 (IT Act) of India, the requirement for a document to be in its "original" form is satisfied if the integrity of the information is maintained from the time it was first generated in its final form. |
| Time of dispatch | The time of dispatch of an electronic communication is the time when it leaves an information system or, if the electronic communication has not left an information system, the time when the electronic communication is received. | the Information Technology Act, 2000 (IT Act) (Section 13)  Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator. |
| Time of receipt | The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. | the Information Technology Act, 2000 (IT Act), the time of receipt of an electronic record is addressed, according to Section 13 of the IT Act.  (2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:--  (a) if the addressee has designated a computer resource for the purpose of receiving electronic records,--  (i) receipt occurs at the time when the electronic record enters the designated computer resource; or  (ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;  (b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee. |
| Place of dispatch and receipt | An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business. | the Information Technology Act, 2000 (IT Act), the time of receipt of an electronic record is addressed, according to Section 13 of the IT Act. |
| Invitations to make offers | Advertisement is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance. | No regulation  The Indian Contract Act, 1872, does not explicitly address electronic communications, its principles regarding offers and invitations to offer are applicable to electronic advertisements. The IT Act and DPDP Act further regulate electronic communications and data protection, respectively, ensuring that electronic advertisements comply with legal standards. ASCI's guidelines supplement these laws by promoting ethical advertising practices in the digital realm. |
| Withdrawal due to error | The party that made the error has the right to withdraw the portion of the electronic communication in which the input error was made if:  (a) other party was notified of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and  (b) the party that made the error has not used or received any material benefit or value from the goods or services, if any, received from the other party. | No regulation  In India, the withdrawal or rectification of errors in electronic communications is primarily governed by the Indian Contract Act, 1872, and the Information Technology Act, 2000. Nevertheless, The IT Act provides legal recognition to electronic records and digital signatures but does not explicitly address the withdrawal of electronic communications due to input errors. |

Part III. Electronic signatures

|  |  |  |
| --- | --- | --- |
| UNCITRAL provision | Content of provision | Implementation in your country |
| Signature technology neutrality | The law recognizes any method of creating an electronic signature that satisfies the requirements. | Chapter II 3A (2) The Information Technology ACT, 2000:  For the purposes of this section **any electronic signature or electronic authentication** technique shall be considered reliable |
| Compliance with a requirement for a signature | Where the law requires a signature of a person (either in the form of an obligation or in the form of consequences for the absence of a signature), that requirement is met if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated. | No regulation |
| Reliability of signature | An electronic signature is considered to be reliable if:  (a) The signature creation data are linked to the signatory and to no other person;  (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;  (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and  (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable. | Chapter II 3A Electronic Signature - The Information Technology ACT, 2008 |
| Conduct of the signatory | Signatory shall:  (a) Exercise reasonable care to avoid unauthorized use of its signature creation data;  (b) Without undue delay, notify that the signature creation data have been compromised; or there is a substantial risk that the signature creation data may have been compromised;  (c) Ensure the accuracy and completeness of all material representations that are included in the certificate;  (d) Bear the legal consequences of its failure to satisfy the above mentioned requirements. | Sections 40-42 of The Information Technology ACT, 2008 |
| Conduct of the certification service provider | Certification service provider shall:  (a) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate or that are included in the certificate;  (b) Provide reasonably accessible means that enable a relying party to identify the certification service provider, verify the signatory and its control of the signature creation data at the time when the certificate was issued; and to verify that signature creation data were valid at or before the time when the certificate was issued;  (c) Provide reasonably accessible means that enable a relying party to ascertain:  (i) The method used to identify the signatory;  (ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;  (iii) That the signature creation data are valid and have not been compromised;  (iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;  (v) Whether means exist for the signatory to give notice that the signature creation data have been compromised;  (vi) Whether a timely revocation service is offered;  (d) Bear the legal consequences of its failure to satisfy the above mentioned requirements. | Section 30 of The Information Technology ACT, 2008, INFORMATION TECHNOLOGY (CERTIFYING AUTHORITY) REGULATIONS, 2001 |
| Requirements to certification service providers | In determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:  (a) Financial and human resources, including existence of assets;  (b) Quality of hardware and software systems;  (c) Procedures for processing of certificates and applications for certificates and retention of records;  (d) Availability of information to signatories identified in certificates and to potential relying parties;  (e) Regularity and extent of audit by an independent body;  (f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing;  (g) Any other relevant factor. | INFORMATION TECHNOLOGY (CERTIFYING AUTHORITY) REGULATIONS, 2001  30. Certifying Authority to follow certain procedures.   * (g) Any other relevant factor can be attributed to:   31. Certifying Authority to ensure compliance of the Act, etc.—Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder. |
| Conduct of the relying party | A relying party shall bear the legal consequences of its failure:  (a) To take reasonable steps to verify the reliability of an electronic signature; or  (b) Where an electronic signature is supported by a certificate, to take reasonable steps:  (i) To verify the validity, suspension or revocation of the certificate; and  (ii) To observe any limitation with respect to the certificate. | No notification about relying party |
| Recognition of foreign certificates and electronic signatures | A certificate issued or an electronic signature created or used outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate (or signature) issued (created or used) in [the enacting State] if it offers a substantially equivalent level of reliability.  In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability, regard shall be had to recognized international standards and to any other relevant factors. Where parties agree to use certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law. | THE INFORMATION TECHNOLOGY ACT, 2000. Chapter IV. 19. Recognition of foreign Certifying Authorities, Information Technology (Recognition of Foreign Certifying Authorities operating under Regulatory Authority ) Regulation 2013 |

Part IV. Identity and trust services

no regulation, UNCITRAL regulation, alternative regulation

|  |  |  |
| --- | --- | --- |
| UNCITRAL provision | Content of provision | Implementation in your country |
| E-identification and identity proofing | Where the law requires the identification of a person, or provides consequences for the absence of identification, that requirement is met with respect to identity management services if a reliable method is used for the identity proofing and electronic identification. | **Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016**: Commonly known as the Aadhaar Act, this legislation establishes the Unique Identification Authority of India (UIDAI) and outlines the process for issuing unique identification numbers (Aadhaar) to residents. It mandates the collection of biometric and demographic data to authenticate identities for accessing various services and subsidies.  **Digital Personal Data Protection (DPDP) Act, 2023**: This recent act introduces comprehensive guidelines for the collection, processing, storage, and transfer of digital personal data. It emphasizes the protection of personal data and outlines the responsibilities of entities handling such data, ensuring that identity proofing and electronic identification processes comply with data protection standards.  [dlapiperdataprotection.com](https://www.dlapiperdataprotection.com/index.html?c=IN&t=law&utm_source=chatgpt.com)  **Identity Verification Guidelines by the Controller of Certifying Authorities (CCA)**: These guidelines mandate that Certifying Authorities (CAs) utilize reliable methods for identity proofing, such as biometric-based authentications, to establish the identity of applicants for digital signature certificates.  [cca.gov.in](https://cca.gov.in/sites/files/pdf/guidelines/CCA-IVG.pdf?utm_source=chatgpt.com) |
| Electronic seals | Where the law requires a legal person to affix a seal, or provides consequences for the absence of a seal, that requirement is met if a reliable method is used:  (a) To provide reliable assurance of the origin of the data message; and  (b) To detect any alteration to the data message after the time and date of affixation, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display. | No regulation |
| Electronic timestamps | Where the law requires a document, record, information or data to be associated with a time and date, or provides consequences for the absence of a time and date, that requirement is met if a reliable method is used:  (a) To indicate the time and date, including by reference to the time zone; and  (b) To associate that time and date with the data message. | Implemented  established by the Information Technology Act, 2000 (IT Act).  Legal Recognition of Electronic Records and Signatures. Section 4, Section 5  Time Stamping Services: The IT Act mandates that Certifying Authorities (CAs) provide time stamping services to ensure the authenticity and integrity of electronic records. The Controller of Certifying Authorities (CCA) oversees the implementation of these services. [cca.gov.in](https://cca.gov.in/time_stamping_service.html?utm_source=chatgpt.com)  Guidelines for Time Stamping. The CCA has issued specific guidelines detailing the operational and technical requirements for time stamping services |
| Electronic archiving | Where the law requires a document, record or information to be retained, or provides consequences for the absence of retention, that requirement is met if a reliable method is used:  (a) To make the information contained in the data message accessible so as to be usable for subsequent reference;  (b) To indicate the time and date of archiving and associate that time and date with the data message;  (c) To retain the data message in the format in which it was generated, sent or received, or in another format which can be demonstrated to detect any alteration to the data message after that time and date, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and  (d) To retain such information, if any, as enables the identification of the origin and destination of a data message and the time and date when it was sent or received. | established by the  Information Technology Act, 2000 (IT Act)  Retention of Electronic Records (Section 7). conditions:   * Accessibility: The information must remain accessible and usable for subsequent reference * Format Integrity: The electronic record should be retained in its original format or in a format that accurately represents the information originally generated, sent, or received. * Metadata Preservation: Details facilitating the identification of the origin, destination, date, and time of dispatch or receipt of the electronic record must be preserved.   Digital Personal Data Protection (DPDP) Act, 2023: emphasizes the principles of data minimization and storage limitation. It mandates that personal data should not be retained beyond the period necessary for achieving the purpose for which it was collected, unless required by law.    Best Practices and Guidelines for Production of Preservable e-Records: Issued by the Ministry of Electronics and Information Technology  Record Retention Schedule: The Government of India's retention schedule outlines the duration for which various categories of records should be maintained. It includes provisions for electronic records |
| Electronic registered delivery services | Where the law requires a document, record or information to be delivered by registered mail or similar service, or provides consequences for the absence of delivery, that requirement is met if a reliable method is used:  (a) To indicate the time and date when the data message was received for delivery and the time and date when it was delivered;  (b) To detect any alteration to the data message after the time and date when the data message was received for delivery to the time and date when it was delivered, apart from the addition of any endorsement or information required by this article, and any change that arises in the normal course of communication, storage and display; and  (c) To identify the sender and the recipient. | No regulation |
| Website authentication | Where the law requires website authentication, or provides consequences for the absence of website authentication, that requirement is met if a reliable method is used:  (a) To identify the person who holds the domain name for the website; and  (b) To associate that person to the website. | no specific legislation mandating website authentication  **Trade Marks Act, 1999:** Although India lacks specific legislation exclusively for domain names, the Trade Marks Act provides protection to domain names as they function as business identifiers.  **Guidelines for Indian Government Websites (GIGW)** |
| Ex post recognition of reliability | The method shall be deemed to be as reliable as appropriate if proven in fact by or before a court or competent adjudicative body to have fulfilled the designated function, by itself or together with further evidence.  In determining the reliability of the method, all relevant circumstances shall be taken into account, which may include compliance with the legal requirements or any applicable recognized international standards and procedures relevant for the provision of the service, as well as any supervision or certification provided with regard to the service. | **Information Technology Act, 2000 (IT Act)** |
| Ex ante designation | A [person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent] may designate identity management or trust services that are presumed reliable. | the **Information Technology Act, 2000 (IT Act).** The Central Government appoints the Controller of Certifying Authorities (CCA) under Section 17 of the IT Act. As per Section 24 of the IT Act, entities seeking to operate as Certifying Authorities must obtain a license from the CCA.  **Digital Personal Data Protection (DPDP) Act, 2023** |
| Obligations in case of data breach | If a breach of security or loss of integrity occurs that has a significant impact on a service, the service provider shall, in accordance with the law:  (a) Take all reasonable steps to contain the breach or loss, including, where appropriate, suspending or revoking the affected service;  (b) Remedy the breach or loss; and  (c) Notify the breach or loss. | **Digital Personal Data Protection (DPDP) Act, 2023**, and directives issued by the **Indian Computer Emergency Response Team (CERT-In)**. |
| Cross-border recognition | The result deriving from the use of an identity management or trust service provided outside [the enacting jurisdiction] shall have the same legal effect in [the enacting jurisdiction] as the result deriving from the use of an identity management or trust service provided in [the enacting jurisdiction] if the method used by the service offers:  (a) At least an equivalent level of reliability, where the reliability levels recognized by such jurisdictions are identical; or  (b) Substantially equivalent or higher level of reliability, in all other cases.  For the purposes of determining the reliability level regard shall be had to recognized international standards. The identity management or trust service shall be presumed to be reliable if [the person, organ or authority specified by the enacting jurisdiction] has ex ante determined the equivalence. | THE INFORMATION TECHNOLOGY ACT, 2000. Chapter IV. 19. Recognition of foreign Certifying Authorities, Information Technology (Recognition of Foreign Certifying Authorities operating under Regulatory Authority ) Regulation 2013 |

Part V. Automated contracting

no regulation, UNCITRAL regulation, alternative regulation

|  |  |  |
| --- | --- | --- |
| UNCITRAL provision | Content of provision | Implementation in your country |
| Legal recognition of automated contracting | A contract formed using an automated system shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in any action carried out in connection with the formation of the contract  An action carried out by an automated system in connection with the formation or performance of a contract shall not be denied legal effect, validity or enforceability on the sole ground that no natural person reviewed or intervened in the action. | 10A The Information Technology ACT, 2008 |
| Computer code and dynamic information | A contract shall not be denied validity or enforceability on the sole ground that the terms of the contract are contained in data messages in the form of computer code.  A contract or an action in connection with it shall not be denied validity or enforceability on the sole ground that it is based on information from a data source that provides information that changes periodically or continuously. | 10A The Information Technology ACT, 2008 + 65B. Admissibility of electronic records. – |
| Attribution of actions carried out by automated systems | As between the parties to a contract, an action carried out by an automated system is attributed in accordance with a procedure agreed to by the parties. If this does not apply, an action carried out by an automated system is attributed to the person who uses the system for that purpose. | IV. Attribution, acknowledgment and dispatch of electronic records. The Information Technology ACT, 2008    Yes, An electronic record shall be attributed to the originator by an information system programmed by or on behalf of the originator to operate automatically. |
| Unexpected actions carried out by automated systems | Unless otherwise agreed by the parties, where an action carried out by an automated system is attributed to a party to a contract, the other party to the contract is not entitled to rely on that action if:  (a) The party to which the action is attributed could not reasonably have expected the action; and  (b) The other party knew or could reasonably be expected to have known that the party to which the action is attributed did not expect the action. | No regulation |
| Non-avoidance | Unless otherwise provided by law, a party shall not be relieved from the legal consequences of its failure to comply with a rule of law on the sole ground that it used an automated system. | Implemented |

Part VI. Electronic transferrable records

no regulation, UNCITRAL regulation, alternative regulation

|  |  |  |
| --- | --- | --- |
| UNCITRAL provision | Content of provision | Implementation in your country |
| Transferable documents or instruments | Where the law requires a transferable document or instrument, that requirement is met by an electronic record if:  (a) The electronic record contains the information that would be required to be contained in a transferable document or instrument; and  (b) A reliable method is used:  (i) To identify that electronic record as the electronic transferable record;  (ii) To render that electronic record capable of being subject to control from its creation until it ceases to have any effect or validity; and  (iii) To retain the integrity of that electronic record. | Implemented only for:  2 [(a) “a cheque in the electronic form” means a cheque drawn in electronic form by using any computer resource and signed in a secure system with **digital signature** (with or without biometrics signature) and asymmetric crypto system or with electronic signature, as the case may be;]  (b) “a truncated cheque” means a cheque which is truncated during the course of a clearing cycle, either by the clearing house or by the bank whether paying or receiving payment, immediately on generation of an electronic image for transmission, substituting the further physical movement of the cheque in writing  Chapter ii (6) THE NEGOTIABLE INSTRUMENTS ACT, 1881 |
| Control | Where the law requires or permits the possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used:  (a) To establish exclusive control of that electronic transferable record by a person; and  (b) To identify that person as the person in control. | They use identification rules of e-signature |
| Transfer | Where the law requires or permits transfer of possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record through the transfer of control over the electronic transferable record. | No regulation |
| Endorsement | Where the law requires or permits the endorsement in any form of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if the information required for the endorsement is included in the electronic transferable record and that information is compliant with the requirements. | No regulation |
| Amendment | Where the law requires or permits the amendment of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used for amendment of information in the electronic transferable record so that the amended information is identified as such. | No regulation |

**Part VII. Other issues**

Please identify the three most important issues related to the electronic commerce or digital trade that are not covered by UNCITRAL documents, but are or will be regulated in your country:

1.Data Protection. India has specific regulations regarding data localization, such as the Reserve Bank of India's mandate for payment data to be stored within India. There are chances for a change in this respect as strong restrictions on data protection is a handicap for e-commerce.

2.[The Digital Personal Data Protection Act 2023](https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf) allows some cross-border data transfers but with certain restrictions, including the government's authority to specify countries where transfers are not permitted. With the development of trade links with appropriate countries the situation can change.

3. IT Act and associated rules.

1. https://www.indiacode.nic.in/bitstream/123456789/16939/1/a2019-35.pdf [↑](#footnote-ref-1)
2. https://thc.nic.in/Central%20Governmental%20Rules/Consumer%20Protection%20(E-Commerce)%20Rules,%202020.pdf [↑](#footnote-ref-2)
3. https://www.indiacode.nic.in/bitstream/123456789/2187/2/A187209.pdf [↑](#footnote-ref-3)
4. https://sansad.in/getFile/BillsTexts/RSBillTexts/Asintroduced/13-Indian%20Contract\_sasmit-E29202471208PM.pdf?source=legislation [↑](#footnote-ref-4)
5. https://www.indiacode.nic.in/bitstream/123456789/4892/1/legalmetrology\_act\_2009.pdf [↑](#footnote-ref-5)
6. https://www.indiacode.nic.in/bitstream/123456789/2082/4/a2007-51.pdf [↑](#footnote-ref-6)
7. https://www.meity.gov.in/sites/upload\_files/dit/files/Digital%20India.pdf [↑](#footnote-ref-7)
8. https://www.makeinindia.com/ [↑](#footnote-ref-8)
9. https://www.startupindia.gov.in/ [↑](#footnote-ref-9)
10. https://www.skillindia.gov.in// [↑](#footnote-ref-10)
11. https://www.ibef.org/industry/ecommerce [↑](#footnote-ref-11)
12. https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY= [↑](#footnote-ref-12)
13. https://www.indianemployees.com/gazette-notifications/details/electronic-signature-or-electronic-authentication-technique-and-procedure-rules-2015 [↑](#footnote-ref-13)
14. https://it.tn.gov.in/sites/default/files/2018-10/IT%20Act%20%28Amendments%292008.pdf [↑](#footnote-ref-14)
15. https://registration.uk.gov.in/files/Stamp\_Act\_Eng.pdf [↑](#footnote-ref-15)
16. https://www.appviewx.com/blogs/preparing-for-indias-new-data-protection-act-with-secure-identity-management/ [↑](#footnote-ref-16)
17. https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY= [↑](#footnote-ref-17)
18. https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMTk4NzY= [↑](#footnote-ref-18)
19. https://prsindia.org/files/bills\_acts/bills\_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf [↑](#footnote-ref-19)
20. https://www.meity.gov.in/writereaddata/files/downloads/National\_cyber\_security\_policy-2013%281%29.pdf [↑](#footnote-ref-20)
21. https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY= [↑](#footnote-ref-21)
22. https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Certifying%20Authority%29.pdf [↑](#footnote-ref-22)
23. https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY= [↑](#footnote-ref-23)
24. https://www.medianama.com/2020/05/223-net-neutrality-india-rules-enforcement/ [↑](#footnote-ref-24)
25. https://pdfs.semanticscholar.org/424a/8ffdc0de57f1fbe1c3a431652deff3fec094.pdf [↑](#footnote-ref-25)