INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CRIMINAL LIABLIITY UNDER INFORMATION ACT 2000 – CHALLENGES, GAPS AND ENFORCEMENT IN THE DIGITAL AGE

AUTHOR – HIMANSHI SINGH, STUDENT AT AMITY UNIVERSITY, NOIDA

BEST CITATION – HIMANSHI SINGH, CRIMINAL LIABLIITY UNDER INFORMATION ACT 2000 – CHALLENGES, GAPS AND ENFORCEMENT IN THE DIGITAL AGE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (5) OF 2026, PG. 601-615, APIS – 3920 – 0001 & ISSN - 2583-2344.

OBJECTIVES, SCOPE, AND APPLICABILITY OF THE IT ACT, 2000

Objectives of the Information Technology Act, 2000

The facts era Act, 2000 was enacted at a time when India turned into witnessing speedy growth in net utilization and electronic commerce. The absence of a selected criminal framework to govern digital transactions and cyber activities made it vital for the legislature to introduce a comprehensive regulation addressing those emerging issues. The Act, therefore, targets to alter digital communication, ensure felony reality, and offer safeguards in opposition to misuse of virtual technology.10The primary objectives of the Act are discussed under.

I. Legal Recognition of Electronic Transactions

One of the primary objectives of the IT Act is to accord legal recognition to electronic recorts, electronic contracts, and digital signatures. By doing so, the Act removes doubts regarding

the validity and enforceability of transactions carried out through electronic means. This recognition has played a significant role in promoting e-commerce, online banking, and electronic filing systems in government departments.

II. Prevention and Control of Cybercrime

some other important goal of the Act is to prevent and manipulate cybercrime. The Act

defines various cyber offences such as unauthorized access, records theft, identity fraud, and cyber terrorism, and prescribes penalties and punishments for

the equal. through criminalising such activities, the Act seeks to deter misuse of computers and virtual networks and ensure duty in cyberspace.

III. Promotion of E-Governance

The IT Act encourages the adoption of electronic means in governance by allowing

government authorities to accept, issue, store, and process documents in electronic form. This objective is aimed at improving administrative efficiency, reducing paperwork, and

increasing transparency and accessibility of public services.

IV. Protection of Data and Information

With the growing dependence on digital platforms, protection of data and information has become crucial. The Act seeks to safeguard sensitive personal data and electronic information from unauthorized access, damage, or misuse. Provisions relating to data protection and compensation for negligence reflect the legislative intent to protect individual privacy and data security.

V. Alignment with International Standards

The IT Act is largely based on the UNCITRAL Model Law on Electronic Commerce, 1996. One

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

of its objectives is to harmonize Indian cyber laws with international legal standards, thereby facilitating cross-border electronic transactions and global trade. This alignment helps India participate effectively in the global digital economy.

Scope of the Information Technology Act, 2000

The scope of the Information Technology Act, 2000 is wide and comprehensive, covering various aspects of electronic communication and digital activity. The Act not only deals with electronic transactions but also addresses offences, liabilities, and regulatory mechanisms related to cyberspace.

I Coverage of Electronic Records and Communication

The Act applies to all electronic records, data messages, and online communications

generated, transmitted, or stored through computers, computer systems, and digital devices. This broad coverage ensures that most forms of digital interaction fall within the ambit of the Act.

II Regulation of Cyber Activities

The IT Act regulates a wide range of cyber activities, including online transactions, digital authentication, electronic storage of data, and electronic governance. It provides a structured legal framework for lawful conduct in the digital environment.

III Cyber Offences and Penalties

The Act covers numerous cyber offences such as hacking, identity theft, cyber fraud, data theft, cyber terrorism, and publication of obscene or sexually explicit material online. It prescribes both civil and criminal penalties, reflecting the seriousness of such offences in the digital age.

IV Intermediary Regulation

The Act lays down the duties and liabilities of intermediaries such as internet service

providers, social media platforms, and online marketplaces. At the same time, it provides safe harbour protection to intermediaries who comply with due diligence requirements, thereby balancing regulation with freedom of digital commerce.[1]

V Adjudicatory and Appellate Mechanism

To ensure effective enforcement, the Act establishes adjudicating authorities and provides for appellate mechanisms for the resolution of cyber disputes. This specialised framework aims to ensure speedy and efficient disposal of cases involving electronic evidence and cyber contraventions.

VI Applicability of the Information Technology Act, 2000

The applicability of the IT Act determines the extent of its jurisdiction and the persons and activities covered under it. The Act adopts a broad approach to ensure effective regulation of cyber activities.

VII Territorial Applicability

The IT Act extends to the whole of India and applies to all offences or contraventions committed within Indian territory. This ensures uniform application of cyber law across the country.

VIII Extra-Territorial Jurisdiction

Under Section 75 of the Act, its provisions apply even to offences committed outside India, provided the computer system or network involved is located in India. This provision reflects the borderless nature of cybercrime and strengthens India's ability to deal with cross-border cyber offences.

Applicability to Individuals and Corporate Bodies

The Act applies to individuals, companies, government bodies, and corporate entities engaged in electronic transactions or cyber activities. This inclusive approach ensures that both natural and legal persons are accountable for cyber offences.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

I. Applicability to Intermediaries

Intermediaries are specifically covered under the Act and are required to observe due

diligence while discharging their functions. Compliance with these obligations enables them to claim safe harbour protection under the law.[2]

II. Exclusions under the Act

Despite its wide applicability, the Act excludes certain documents such as wills, power of

attorney, trust deeds, and negotiable instruments from its ambit. These exclusions reflect the legislature's intention to retain traditional legal formalities for specific categories of documents.

Legal Recognition of Electronic Records and Digital Signatures

The legal recognition of electronic records and digital signatures constitutes the foundation of the Information Technology Act, 2000. Before the enactment of this legislation, Indian law primarily recognised paper-based documents and handwritten signatures as valid means of legal communication. With the rapid expansion of information technology, electronic commerce, and digital governance, this traditional approach proved inadequate. It became essential to provide legal legitimacy to electronic forms of communication to ensure certainty, reliability, and enforceability in digital transactions. The IT Act was thus enacted to bridge this legal vacuum and to place electronic records and digital signatures on the same legal footing as conventional documents.

Concept of Electronic Records

An digital file refers to any facts, document, or statistics generated, received, transmitted, or saved in digital shape. segment 2(1)(t) of the records era Act, 2000 defines an digital document as statistics recorded or stored in magnetic, optical, computer memory, microfilm, or similar devices. This expansive definition displays the legislature's intention to cover all present and future forms of digital data, irrespective of the medium used for storage.[3]

In a modern digital society, communication and documentation largely take place through emails, online portals, cloud storage, and electronic databases. The legal recognition of electronic records ensures that such digital information can be relied upon for official, commercial, and legal purposes, thereby reducing dependence on physical documentation and manual processes.

Legal Validity of Electronic Records

section 4 of statistics generation Act,2000 offers statutory popularity to electronic facts via s upplying that in which any regulation calls for facts to be in writing or revealed form, such requirement will be deemed to were fulfilled if the records is

made available in digital shapeand is accessible for subsequent reference. This provision eliminates the traditional preference for paper-based records and establishes functional equivalence between electronic and physical documents.[4]

The significance of this provision lies in its practical application. Contracts executed online, electronic notices, digital invoices, and electronically maintained records are legally valid, provided they comply with the conditions laid down under the Act. This has greatly

facilitated the growth of e-commerce, digital banking, and electronic administration in India.

Electronic Records and Evidence Law

The recognition of electronic records has also brought about significant changes in the law of evidence. Section 65B of the Indian Evidence Act, 1872, introduced through the IT Act,

provides that electronic records are admissible as evidence in judicial proceedings, subject to compliance with prescribed conditions. This inclusion allows courts to rely on emails, call records, digital documents, and electronic logs while adjudicating disputes.[5]

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

At the same time, the law imposes safeguards to ensure authenticity and reliability. The requirement of a certificate under Section 65B aims to prevent tampering, fabrication, and misuse of electronic evidence. Thus, while electronic records are legally recognised, their evidentiary value depends upon compliance with procedural requirements, thereby balancing technological advancement with judicial caution.

Concept of Digital Signatures

In nowadays's virtual world, wherein maximum verbal exchange and transactions manifest on-line, ensuring that statistics is real and at ease has end up extraordinarily important. digital signatures play a

key position in accomplishing this via providing a reliable manner to confirm the identity of the sender and to ensure that the content of a document has now not been altered at some stage in transmission.

A virtual signature may be understood as an advanced shape of an electronic signature that uses cryptographic techniques to confirm the authenticity of a digital message

or document. not like a scanned handwritten signature or a typed name,

a virtual signature gives a much better degree of safety. it works at the concept of public key infrastructure (PKI), which involves two keys—a non-public key and a public key. The

sender makes use of their non-public key to signal the report, while the receiver uses the corresponding public key to confirm it.

This manner guarantees 3 essential factors of digital communique: authenticity (confirming the identification of the sender), integrity (making sure the content has not been modified), and non-repudiation (stopping the sender from denying the transaction).

In India, digital signatures are legally recognized below the statistics generation Act, 2000. The Act presents a felony framework for the use of virtual signatures and defines them as a technique of authenticating electronic facts. It also regulates the issuance

of digital Signature certificates (DSCs) through Certifying government, which can

be chargeable for verifying the identification of individuals and companies before granting such certificate.

digital signatures are broadly used in numerous sectors today. They play

an important position in e-commerce, on-line banking, governance services, filing profits tax returns, and even in executing digital contracts. by way of ensuring at

ease and honest transactions, they assist in building self-fraud. however, despite their many benefits, there are nonetheless a few demanding situations associated

with virtual signatures. Many users are not fully aware about how they paintings, and the technical components can occasionally be difficult to understand. There also

are concerns about the misuse of personal keys,the threat ounauthorized access. moreover, as technology continues to conform, it will become essential to regularly replace felony and regulatory frameworks to hold the security and effectiveness of digital signatures.

Legal Recognition of Digital Signatures

Section 5 of the Information Technology Act, 2000 accords legal recognition to digital signatures by stating that where any law requires a signature, such requirement shall be

satisfied if the document is authenticated using a digital signature in the prescribed manner. This provision effectively places digital signatures on par with handwritten signatures.

The legal recognition of digital signatures has enabled the execution of contracts, filing of tax returns, submission of government forms, and conduct of e-tendering through electronic means. It has significantly contributed to the efficiency and transparency of electronic governance and commercial transactions.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Secure Electronic Records and Secure Digital Signatures and Role of Certifying Authorities

In today's digital world, where most communication and transactions take place online, it is not enough to simply create electronic records or use digital signatures. It is equally

important that they are secure and reliable. These elements are essential for building trust and ensuring that digital transactions are legally valid.

A secure electronic record is one that is protected from unauthorized access or any kind of alteration. Under the Information Technology Act, 2000, an electronic record is considered secure if it has been properly authenticated and remains unchanged, which makes it dependable as legal evidence.

In the same way, a secure digital signature is created through a secure system and is uniquely connected to the signer. It remains under the signer's control and is designed in such a way that any change in the document can be detected.[6] This helps ensure authenticity, integrity, and prevents the signer from denying their involvement.

Certifying Authorities (CAs) play an important role in this system by issuing Digital Signature Certificates (DSCs) after verifying the identity of individuals or organizations. They act as trusted intermediaries, making digital transactions safer and more reliable. These authorities are supervised by the Controller of Certifying Authorities (CCA), which ensures that they follow proper legal and technical standards.[7]

Overall, secure electronic records and digital signatures give legal recognition and

evidentiary value to online transactions. However, challenges such as technical risks and lack of awareness still exist. Together with the role of Certifying Authorities, they form the backbone of a secure and trustworthy digital system.

Electronic Contracts and Digital Authentication its Limitations and Exclusions

In today's digital economy, contracts are no longer confined to paper. With the rise of e-commerce and online platforms, electronic contracts (e-contracts) have become a common way of entering into legally binding agreements. These contracts are formed through emails, websites, and mobile applications, making transactions quicker and more convenient.

An e-contract is essentially the digital version of a traditional contract and follows the same basic principles such as offer, acceptance, and lawful consideration. In India, their validity is recognized under the Information Technology Act, 2000, which gives legal recognition to electronic records and digital signatures, provided the conditions of the Indian Contract Act, 1872 are fulfilled.

A crucial aspect of e-contracts is digital authentication, which helps verify the identity of parties and confirm their consent. This is commonly done through digital signatures,

electronic signatures, or OTP-based verification. Such methods ensure authenticity, integrity, and trust in online transactions.

However, these systems are not without challenges. Risks such as fraud, identity theft, and unauthorized access can undermine their reliability. Many users also agree to "click-wrap" contracts without fully understanding the terms, raising concerns about informed consent. Additionally, technical issues like system failures or cyberattacks can further weaken the effectiveness of digital authentication.

There are also legal limitations, particularly in proving electronic evidence in court and dealing with cross-border jurisdiction issues. Moreover, the law excludes certain

documents—such as wills, powers of attorney, trust deeds, and contracts for the sale of

immovable property—from electronic

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

recognition, requiring them to be executed in physical form.[8]

In conclusion, while electronic contracts and digital authentication have made transactions more efficient and accessible, their limitations and exclusions highlight the need for stronger safeguards and continuous legal development.

Significance in the Digital Age

The legal recognition of electronic records and digital signatures has fundamentally transformed India's legal, commercial, and administrative framework. It has reduced procedural delays, minimised paperwork, and facilitated transparency and efficiency in governance and trade. In an era marked by digital transactions and global connectivity, such recognition is indispensable.

Nevertheless, challenges such as cyber fraud, identity theft, and technological vulnerabilities persist. Therefore, while the IT Act provides a strong legal foundation, continuous legal reform and technological advancement are necessary to sustain trust in electronic systems.

IMPORTANT PROVISIONS AND STRUCTURE ACT

The Information Technology Act, 2000 serves as the cornerstone of India's cyber law framework. Enacted at a time when digital technology was rapidly transforming modes of communication and commerce, the Act was designed to address the legal vacuum surrounding electronic transactions and cyber activities in India. It not only facilitates the growth of e-commerce and e-governance but also establishes a robust mechanism to deter cyber offences and regulate digital conduct. The structure of the Act reflects a dual

objective—promotion of digital innovation on one hand and prevention of misuse of technology on the other.

Overall Structure of the Information Technology Act, 2000

The Information Technology Act, 2000 is India's primary law governing electronic transactions, digital signatures, and cyber offences. It was enacted to promote e-commerce and give legal recognition to electronic records, forming a comprehensive framework for activities in cyberspace.

The Act begins with preliminary provisions defining key terms and its scope. It then grants legal recognition to electronic records and digital signatures, placing them on the same footing as traditional paper-based transactions.

It further regulates digital signatures and establishes Certifying Authorities, which issue Digital Signature Certificates to ensure authenticity in digital communications.

A major part of the Act deals with cyber offences and penalties, covering offences like unauthorized access, data theft, and fraud, along with provisions for adjudication and compensation.[9]It also provides for appellate mechanisms and grants powers to law enforcement agencies for investigation and enforcement.[10]

The Act addresses intermediary liability, offering limited immunity to platforms subject to due diligence, as clarified in *Shreya Singhal v. Union of India*.

In conclusion, the Act provides a structured legal framework for cyberspace but requires continuous updates to remain effective in the rapidly evolving digital landscape.

Preliminary Provisions (Chapter I: Sections 1–2)

Chapter I lays the foundation of the Act by dealing with its short title, extent, commencement, and definitions. Section 1 extends the Act to the whole of India and, when read with Section 75, confers extra-territorial jurisdiction, recognising the inherently borderless nature of cyber activities.

Section 2 assumes critical importance as it defines essential terms such as *computer*,

computer system, *computer network*, *data*, *electronic record*, *digital signature*, *intermediary*, and *cyber café*. These definitions

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

determine the scope and applicability of the Act and play a decisive role in judicial interpretation. The legislature has deliberately adopted technology- neutral and expansive definitions, enabling the Act to remain relevant despite rapid technological evolution.[11]

2.2.1 Legal Recognition of Electronic Records and Digital Signatures

(Chapter II: Sections 3–10A)

Chapter II constitutes the core of the Information Technology Act, as it grants legal

recognition to electronic records and digital signatures. Section 3 introduces digital signatures based on asymmetric cryptography and hash functions, ensuring authenticity and integrity of electronic records.

Section 4 accords legal recognition to electronic records by providing that information shall not be denied legal effect merely because it is in electronic form. Section 5 similarly recognises digital signatures, placing them on par with handwritten signatures. These provisions remove long-standing legal barriers to electronic commerce.

Sections 6 and 7 promote electronic governance by permitting government authorities to accept, issue, retain, and store documents electronically. Section 8 further validates the electronic publication of official rules, regulations, and notifications.

A landmark provision, Section 10A, introduced by the 2008 Amendment, clarifies that contracts formed through electronic means shall not be deemed unenforceable solely because electronic communication was used. This provision has significantly strengthened the legal foundation of online contracts, click-wrap agreements, and digital marketplaces.

Regulation of Certifying Authorities and Electronic Governance

(Chapter III: Sections 17–34)

Chapter III establishes a statutory framework for regulating digital authentication through **Certifying Authorities (CAs)**. It provides for the appointment of the **Controller of Certifying Authorities (CCA)**, who exercises regulatory and supervisory control over licensed certifying authorities.[12]

The provisions of this chapter deal with:

- Licensing and regulation of certifying authorities
- Issuance, suspension, and revocation of Digital Signature Certificates
- Duties and responsibilities of certifying authorities
- Maintenance of secure repositories of digital certificates

By ensuring accountability and standardisation in digital certification, this chapter enhances public confidence in electronic transactions and authentication system

(Chapter IV: Sections 5–8)

The electronic governance provisions facilitate the transformation of traditional administrative processes into digital formats. These provisions enable electronic filing of documents, online payment of fees, and electronic communication between government departments and citizens.

The significance of these provisions lies in their contribution to administrative efficiency, transparency, and accessibility. They laid the statutory groundwork for major initiatives such as Digital India, online tax filing systems, electronic procurement (e-tendering), and digital public service delivery platforms.

Civil Liability and Compensation and Cyber Offences and Criminal Liability

(Chapter IX: Sections 43–47)

Chapter IX introduces a civil liability regime to address unauthorised access and damage to computer systems. Section 43 provides for compensation in cases involving unauthorised access, data theft, introduction of viruses, denial-of-service attacks, and damage to computer resources.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

A significant addition through the 2008 Amendment is Section 43A, which imposes liability on body corporates for negligence in implementing reasonable security practices resulting in wrongful loss or gain. This provision plays a vital role in promoting corporate responsibility, data security, and consumer trust in the digital ecosystem.[13]

(Chapter XI: Sections 65–74)

Chapter XI deals with criminal offences under the Act and reflects the legislature's intent to combat cybercrime effectively. It criminalises acts such as:

- Tampering with computer source documents (Section 65)
- Computer-related offences (Section 66)
- Identity theft (Section 66C)
- Cheating by personation using computer resources (Section 66D)
- Violation of privacy (Section 66E)
- Cyber terrorism (Section 66F)

Sections 67, 67A, and 67B address the publication and transmission of obscene material, sexually explicit content, and child sexual abuse material in electronic form. These provisions underscore the State's obligation to protect public morality, dignity, and vulnerable groups in cyberspace.

Adjudication and Appellate Mechanism

(Chapter X: Sections 46–62)

To ensure speedy and specialised dispute resolution, the Act establishes an adjudicatory mechanism under Section 46, empowering adjudicating officers to decide matters involving compensation claims.

Appeals against such decisions were originally heard by the Cyber Appellate Tribunal, which has since been merged with the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). This specialised mechanism reduces the burden on conventional courts and promotes technical expertise in cyber dispute resolution.

Intermediary Liability

(Section 79)

Section 79 provides conditional safe harbour protection to intermediaries such as internet service providers, social media platforms, and online marketplaces. Intermediaries are exempt from liability for third-party content provided they observe due diligence and do not knowingly facilitate unlawful activity.

This provision seeks to strike a delicate balance between innovation, freedom of expression, and accountability, and has been the subject of extensive judicial interpretation and policydebate.

Powers of Investigation and Enforcement

(Chapter XII: Sections 69–78)

The Act confers significant powers on the government for investigation and enforcement. Section 69 authorises interception, monitoring, and decryption of information in the interest of national security, sovereignty, and public order.

Sections 70 and 70B deal with protected systems and the functions of the Indian Computer Emergency Response Team (CERT-In). Section 80 empowers police officers to conduct searches and make arrests without warrant in specified circumstances. While these provisions strengthen cyber enforcement, they have also raised concerns regarding privacy and proportionality.

Amendments Introduced by the Information Technology (Amendment) Act, 2008

The rapid expansion of information and communication technology in the early years of the twenty-first century fundamentally transformed the way individuals, commercial entities, and governments interacted and conducted transactions. Digital platforms became central to communication, commerce, and governance. Although the Information Technology Act, 2000 was a pioneering piece of

legislation that granted legal recognition to electronic records and digital signatures, it soon became apparent that the Act was insufficient to deal with emerging

cyber threats, sophisticated cybercrimes, data protection concerns, and the growing role of online intermediaries. The original legislation was largely facilitative in nature, focusing primarily on e-commerce and e-governance, with limited emphasis on cyber security and criminal misuse of technology.

Recognising these shortcomings, the Indian legislature enacted the **Information Technology (Amendment) Act, 2008**, which came into force on 27 October 2009. The amendment

marked a decisive shift in India's cyber law framework by strengthening provisions relating to cyber offences, data protection, electronic authentication, intermediary liability, and national cyber security. It transformed the IT Act from a largely enabling statute into a comprehensive regulatory and penal law capable of addressing the complexities of the digital age[14].

Objectives of the IT (Amendment) Act, 2008

The primary objective of the 2008 Amendment was to modernise the existing legal framework in response to rapid technological advancements and the increasing incidence of cybercrime. The Statement of Objects and Reasons accompanying the amendment emphasised the need to address new and sophisticated forms of cyber offences, protect sensitive personal data, and strengthen mechanisms for national cyber security.

Another significant objective was to harmonise Indian cyber laws with international legal standards, particularly the **UNCITRAL Model Law on Electronic Signatures**, thereby

facilitating cross-border electronic transactions and global digital trade. At the same time, the amendment sought to strike a careful balance between encouraging technological innovation and ensuring regulatory oversight, so that legitimate online activities were protected while misuse of digital platforms was effectively penalised.

Introduction of Electronic Signatures

One of the most significant reforms introduced by the 2008 Amendment was the replacement of the limited concept of digital signatures with the broader and technology-neutral concept of **electronic signatures**. Under the original Act, authentication of electronic records was restricted to digital signatures based on asymmetric cryptography, which soon became technologically restrictive.

To overcome this limitation, the amendment introduced **Section 3A**, which provides legal recognition to electronic signatures that are considered reliable and secure. This change enabled the legal acceptance of diverse authentication technologies such as biometric

identifiers, smart cards, and other emerging methods. By adopting a technology-neutral approach, the legislature ensured that the Act remained flexible and adaptable to future technological developments without the need for frequent amendments.

Expansion of Cyber Offences and Criminal Liability

The 2008 Amendment substantially expanded the scope of cyber offences under the Act.

While Section 66 existed in the original legislation, it was inadequate to address complex and evolving forms of cybercrime. The amendment introduced several new offences to deal with emerging patterns of cyber misconduct[15].

Identity Theft (Section 66C)

Section 66C criminalises identity theft, including the dishonest or fraudulent use of another person's password, digital signature, or unique identification feature. This provision directly addresses crimes such as phishing, unauthorised account access, and online impersonation[11].

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Cheating by Personation (Section 66D)

Section 66D deals specifically with cheating by personation through computer resources. It has become particularly relevant in cases involving online fraud, fake profiles, and financial scams conducted through digital platforms.

Violation of Privacy (Section 66E)

Section 66E penalises the intentional capturing, publishing, or transmission of private images without consent. This provision plays a vital role in addressing offences such as voyeurism, revenge pornography, and other serious violations of individual privacy in cyberspace.

Cyber Terrorism (Section 66F)

Section 66F, one of the most stringent provisions introduced by the amendment, defines and punishes cyber terrorism. It covers acts that threaten the sovereignty, integrity, security, or public order of the nation through unauthorised access to computer systems or networks. This provision reflects the growing recognition of cyberspace as a potential domain for national security threats.

Data Protection and Corporate Accountability

A major deficiency in the original IT Act was the absence of clear provisions relating to data protection and corporate responsibility. The 2008 Amendment addressed this gap by

introducing **Section 43A**, which imposes liability on body corporates for negligence in implementing reasonable security practices.

Under this provision, if a company handling sensitive personal data fails to maintain adequate security safeguards and causes wrongful loss or gain, it is liable to pay compensation. This marked India's first statutory recognition of corporate responsibility in data protection matters. To give practical effect to Section 43A, the government subsequently notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, thereby laying the foundation for modern data protection jurisprudence in India.

Intermediary Liability and Safe Harbour Protection

Another transformative reform introduced by the 2008 Amendment was the revision of **Section 79**, which governs intermediary liability. The original provision lacked clarity and exposed intermediaries to excessive and uncertain legal risks.

The amended Section 79 grants conditional safe harbour protection to intermediaries such as internet service providers, social media platforms, search engines, and online marketplaces. Intermediaries are exempt from liability for third-party content provided they observe due diligence and do not knowingly facilitate unlawful activity. Judicial interpretation,

particularly in *Shreya Singhal v. Union of India*, clarified that intermediaries are required to act only upon receiving actual knowledge through a court order or government notification[16].

Strengthening Government Powers of Interception and Monitoring

The amendment significantly enhanced the government's powers to intercept, monitor, and decrypt electronic information. **Section 69** authorises such actions in the interests of national security, sovereignty, and public order. Additionally, **Sections 69A and 69B** were introduced to regulate blocking of online content and monitoring of internet traffic.

While these provisions strengthen cyber security and national interests, they have also

generated concerns regarding excessive surveillance and potential infringement of the right to privacy. Courts have therefore emphasised the need for procedural safeguards and proportionality in the exercise of these powers.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Protection of Critical Information Infrastructure

The 2008 Amendment introduced Sections 70 and 70A, empowering the government to declare certain computer resources as protected systems. Unauthorised access to such systems attracts stringent penalties. Section 70A provides for the establishment of the National Critical Information Infrastructure Protection Centre (NCIIPC), tasked with safeguarding vital sectors such as banking, power, telecommunications, and defence. This reflects the increasing recognition of cyber security as an integral component of national infrastructure protection.

Establishment of CERT-In

Another significant reform was the statutory recognition of the Indian Computer Emergency Response Team (CERT-In) under Section 70B. CERT-In functions as the national nodal

agency for responding to cyber security incidents, issuing alerts, and coordinating incident response measures[24]. This institutional framework enhances India's capacity to address cyber threats in a coordinated and timely manner.

Changes in Adjudication and Appellate Mechanism

The amendment strengthened the adjudicatory framework by enhancing the powers of adjudicating officers and streamlining appellate procedures. The objective was to ensure

faster and more specialised resolution of cyber disputes. The subsequent merger of the Cyber Appellate Tribunal with the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) further integrated cyber dispute resolution into the broader regulatory structure.

Impact and Criticism of the 2008 Amendment

The IT (Amendment) Act, 2008 significantly strengthened India's cyber law regime by expanding cyber offences, introducing data protection obligations, clarifying intermediary liability, and reinforcing national cyber security mechanisms. However, the amendment has also been criticised for granting wide surveillance powers to the government without sufficiently robust safeguards.

Civil society organisations and legal scholars have raised concerns regarding privacy, freedom of expression, and the potential misuse of interception and monitoring provisions[17]. Despite these criticisms, the amendment remains a landmark development in Indian cyber law and laid the groundwork for subsequent reforms in digital governance and data protection.

Relationship between the Information Technology Act and Other Criminal Laws

The rapid digitalisation of society has gradually blurred the traditional boundaries between physical and virtual spaces. As technology became deeply integrated into daily life, new forms of criminal conduct began to emerge, many of which overlapped with offences already recognised under conventional criminal laws. In India, the Information Technology Act, 2000 does not function in isolation. Instead, it operates alongside traditional criminal statutes such as the Indian Penal Code, 1860 (IPC), the Code of Criminal Procedure, 1973 (CrPC), the Indian Evidence Act, 1872, and several specialised criminal legislations. Together, these laws form a comprehensive legal framework designed to address the increasing complexity of cyber-enabled crimes.

The IT Act was enacted primarily to deal with offences committed through computer systems, digital devices, and electronic networks. However, cyber offences frequently involve elements that are already punishable under general criminal laws. As a result, courts and investigating agencies often apply provisions of the IT Act along with other criminal statutes.

Understanding this relationship is essential for analysing how cybercrime is investigated, prosecuted, and adjudicated within the Indian

criminal justice system.

IT Act and the Indian Penal Code, 1860

The Indian Penal Code, 1860 remains the cornerstone of criminal law in India, defining a wide spectrum of offences including cheating, fraud, forgery, defamation, criminal

intimidation, and obscenity. With the rise of digital technology, many of these traditional offences have acquired a cyber dimension, resulting in significant overlap between the IPC and the IT Act[18].

For example, online cheating and fraud may attract Section 66D of the IT Act, which deals with cheating by personation through computer resources, along with Section 420 IPC, which criminalises cheating and dishonestly inducing delivery of property. Similarly, identity theft under Section 66C of the IT Act often overlaps with offences under Sections 419 and 468 IPC, which relate to impersonation and forgery respectively.

In cases involving online defamation, courts frequently apply Section 499 IPC alongside relevant provisions of the IT Act. Likewise, cyberstalking and online harassment may involve Section 66E of the IT Act, which deals with violation of privacy, in addition to IPC

provisions relating to criminal intimidation and intentional insult.

Indian courts have consistently clarified that the IT Act does not exclude the applicability of the IPC. Instead, both statutes may be invoked simultaneously where the ingredients of offences under both laws are satisfied. This approach ensures that offenders cannot evade liability merely because the offence was committed through digital means.

IT Act and the Code of Criminal Procedure, 1973

The Code of Criminal Procedure, 1973 regulates the procedural aspects of criminal law,

including investigation, arrest, search, seizure, trial, and sentencing. While the IT Act creates substantive offences relating to cyber misconduct, the procedural framework for investigation and prosecution is largely governed by the CrPC.

Sections 78 and 80 of the IT Act empower police officers to investigate cyber offences and conduct search and seizure operations. However, these powers must be exercised in

accordance with procedural safeguards provided under the CrPC. Arrest procedures, remand, filing of charge sheets, and trial processes relating to cyber offences follow the same procedural standards applicable to other criminal offences unless specifically modified by the IT Act.

The classification of offences under the IT Act as cognizable or non-cognizable also

determines the applicability of CrPC provisions. Most serious cyber offences are categorised as cognizable, enabling law enforcement agencies to initiate investigations without prior court approval. This integration promotes procedural consistency and avoids conflicts

between special cyber law provisions and general criminal procedural law[19].

IT Act and the Indian Evidence Act, 1872

Perhaps the most significant interaction between the IT Act and other criminal laws occurs in relation to the Indian Evidence Act, 1872, particularly concerning the admissibility of electronic evidence. Prior to the enactment of the IT Act, the Evidence Act did not adequately recognise electronic records as admissible evidence.

The IT Act introduced Sections 65A and 65B into the Evidence Act, specifically addressing the admissibility and evidentiary value of electronic records. Section 65B establishes the conditions under which electronic records such as emails, call data records, CCTV footage, and digital documents may be produced and relied upon in court proceedings.

Judicial interpretation of these provisions, particularly in *Anvar P.V. v. P.K. Basheer* and

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, reinforced that compliance with Section 65B certification is mandatory for admissibility of electronic evidence. These

decisions illustrate how the IT Act has fundamentally reshaped evidentiary standards in criminal trials involving digital material.

IT Act and Special Criminal Legislations

Apart from general criminal statutes, the IT Act also operates in conjunction with several special legislations addressing specific forms of crime. This relationship is particularly relevant in offences involving online exploitation, financial fraud, and threats to national security.

For instance, offences involving online sexual exploitation of children may attract provisions of the Protection of Children from Sexual Offences Act, 2012 (POCSO) alongside Section

67B of the IT Act, which criminalises child sexual abuse material in electronic form.

Similarly, cyber frauds involving financial transactions may also fall within the ambit of the Prevention of Money Laundering Act, 2002 (PMLA) if proceeds of crime are concealed or laundered through digital platforms.

Cyber offences affecting national security may overlap with the Unlawful Activities (Prevention) Act, 1967 (UAPA), particularly in cases involving cyber terrorism under Section 66F of the IT Act. In such situations, the IT Act supplements specialised legislation by addressing the technological dimension of the offence.

Doctrine of Special Law Prevailing over General Law

The relationship between the IT Act and other criminal laws is guided by the legal principle "generalia specialibus non derogant," which means that special laws prevail over general laws in matters specifically covered by the special statute. The IT Act is regarded as a

specialised legislation dealing with offences involving computers and electronic communication systems.

However, this principle does not automatically exclude the applicability of general criminal laws. Courts have repeatedly held that when an act constitutes offences under both the IT Act and the IPC, prosecution under both statutes is permissible unless explicitly barred. This approach ensures comprehensive criminal liability and serves as an effective deterrent against cybercrime[20].

IT Act and Jurisdictional Issues

Cybercrimes frequently transcend national and territorial boundaries, creating complex jurisdictional challenges. The IT Act addresses this issue through **Section 75**, which extends the Act's applicability to offences committed outside India if the computer system, network, or data involved is located within Indian territory[17].

This provision operates alongside jurisdictional provisions contained in the IPC and CrPC,

which also address offences committed beyond territorial boundaries. Together, these statutes enable Indian courts to exercise jurisdiction over cross-border cyber offences, reflecting the inherently global nature of cybercrime[18].

IT Act and Police Powers

The IT Act supplements the investigative powers available under general criminal law by granting specific authority to deal with cyber offences. **Section 80 of the IT Act** authorises police officers to conduct searches and make arrests without warrant in certain cybercrime cases.

Nevertheless, these powers must be exercised in conformity with constitutional safeguards and procedural protections provided under the CrPC. Judicial oversight ensures that enforcement powers under the IT Act are exercised responsibly and are not misused by investigating authorities.

Judicial Interpretation and Harmonious Construction

Indian courts have consistently applied the principle of **harmonious construction** while

interpreting the IT Act in relation to other criminal statutes. Rather than viewing these laws as conflicting, courts attempt to interpret them in a manner that allows all relevant provisions to operate effectively.

In *Shreya Singhal v. Union of India*, the Supreme Court emphasised the importance of balancing freedom of speech with regulatory oversight under cyber law. Similarly, courts have harmonised provisions of the IT Act with evidentiary rules under the Evidence Act to ensure fairness and reliability in criminal trials. Such judicial interpretation has played a vital role in integrating cyber law into the broader criminal justice framework.

Practical Challenges in Concurrent Application of Laws

Despite the complementary nature of the IT Act and other criminal laws, several practical challenges persist. Investigating agencies often face difficulties in determining the appropriate legal provisions, resulting in overlapping charges or incorrect application of law.

Additionally, lack of specialised technical expertise among law enforcement agencies, delays in digital forensic examination, and inconsistencies in judicial interpretation further

complicate the effective enforcement of cyber laws. These challenges highlight the need for specialised training, improved forensic infrastructure, and clearer legislative guidance to ensure efficient prosecution of cyber offences[21].

FOOTNOTES / REFERENCES

Statutory References

1. Information Technology Act, 2000, § 2(1)(t).
2. Information Technology Act, 2000, § 4.
3. Information Technology Act, 2000, § 5.
4. Information Technology Act, 2000, § 10A.
5. Information Technology Act, 2000, § 43.
6. Information Technology Act, 2000, § 43A.
7. Information Technology Act, 2000, §§ 65–66.
8. Information Technology Act, 2000, §§ 66C–66F.
9. Information Technology Act, 2000, §§ 67–67B.
10. Information Technology Act, 2000, § 69.
11. Information Technology Act, 2000, § 69A.
12. Information Technology Act, 2000, § 70.
13. Information Technology Act, 2000, § 70B.
14. Information Technology Act, 2000, § 75.
15. Information Technology Act, 2000, § 79.
16. Information Technology Act, 2000, §§ 46–62.
17. Information Technology (Amendment) Act, 2008.

Other Statutes

18. Indian Evidence Act, 1872, § 65B.
19. Indian Penal Code, 1860, §§ 419, 420, 468, 499.
20. Code of Criminal Procedure, 1973.
21. Protection of Children from Sexual Offences Act, 2012.
22. Prevention of Money Laundering Act, 2002.
23. Unlawful Activities (Prevention) Act, 1967.

Case Laws

24. Shreya Singhal v. Union of India.
25. Anvar P.V. v. P.K. Basheer.
26. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal.

International Instrument

27. UNCITRAL Model Law on Electronic Commerce, 1996.
28. UNCITRAL Model Law on Electronic Signatures, 2001.

Books & Commentaries (Optional but Recommended for Dissertation)

29. Pavan Duggal, *Cyber Law in India* (LexisNexis).
30. Vakul Sharma, *Information Technology Law and Practice* (Universal Law Publishing).
31. Justice Yatindra Singh, *Cyber Laws* (Universal Law Publishing).

Government Rules & Reports

32. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
33. Ministry of Electronics and Information Technology (MeitY), Government of India – Official Reports on Cyber Law & Policy.

ENDNOTES

1 Section 2(1)(t), Information Technology Act, 2000.

2 Section 4, Information Technology Act, 2000.

3 Section 65B, Indian Evidence Act, 1872.

4 Ibid., Sec. 15.

5 Ibid., Sec. 43, 65–66.

6 S.K. Verma & Raman Mittal, Legal Dimensions of Cyber Space, Indian Law Institute, New Delhi

7 Section 43A, Information Technology Act, 2000; IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

8 S.K. Verma, Cyber Laws and Information Technology, Universal Law Publishing.

9 Sections 66C–66F, IT Act, 2000.

10 Shreya Singhal v. Union of India, (2015) 5 SCC 1.

11 National Crime Records Bureau Cyber Crime Statistics.