INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 12 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 12 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-12-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

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

VOLUME 5 AND ISSUE 12 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

DIGITAL SIGNATURES IN THE ERA OF ICT: CHALLENGES IN CRIMINAL LAW ENFORCEMENT

AUTHOR – DHARANI. S, STUDENT AT TAMILNADU DR.AMBEDKAR LAW UNIVERSITY

BEST CITATION - DHARANI. S, DIGITAL SIGNATURES IN THE ERA OF ICT: CHALLENGES IN CRIMINAL LAW ENFORCEMENT, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (12) OF 2025, PG. 815-821, APIS – 3920 – 0001 & ISSN - 2583-2344

ABSTRACT

In the digital age, the use of Information and Communication Technology (ICT) has become deeply embedded in modern governance, business, and personal interactions. Among the key tools enabling secure electronic communication is the digital signature, a cryptographic mechanism that ensures the authenticity, integrity, and non-repudiation of electronic documents and transactions. Digital signatures have been legally recognized in many jurisdictions and are vital to promoting trust in electronic commerce, e-governance, and legal documentation. However, the rise in digital signature usage has been paralleled by a corresponding increase in cybercrime and misuse, presenting significant challenges for criminal law enforcement agencies. The advent of Information and Communication Technology (ICT) has transformed the way individuals, businesses, and governments interact, especially through digital transactions. At the core of this transformation lies the use of digital signatures, which ensure authentication, integrity, and non-repudiation in electronic communications. While digital signatures offer significant advantages in efficiency and security, their misuse poses considerable challenges to criminal law enforcement. These challenges include jurisdictional complexities, evidentiary issues, lack of technical expertise, and regulatory gaps. This paper explores the multifaceted legal and investigative difficulties posed by digital signature-related crimes, evaluates existing legal frameworks, and proposes potential solutions for more effective enforcement.

Keywords

Digital Signatures, Cybercrime, ICT, Criminal Law Enforcement, Public Key Infrastructure, Electronic Evidence, Jurisdiction, Digital Forensics, Legal Frameworks.

INTRODUCTION

The rapid advancement of Information and Communication Technology (ICT) has revolutionized how individuals, organizations, and governments conduct their daily operations. With the increasing digitization of services, there is a growing reliance on secure electronic transactions and documentation. One of the key components enabling trust in the digital environment is the digital signature - a cryptographic mechanism that authenticates the identity of a signer and ensures the integrity of digital communications. Digital signatures have become indispensable in various sectors, including e-commerce, e-governance, online banking, and legal documentation. They offer essential features such as authentication, data integrity, and non-repudiation, making them legally recognized in many jurisdictions under acts like the Information Technology Act, 2000 (India), eIDAS Regulation (EU), and ESIGN Act (USA). Despite their benefits, digital signatures are not immune to misuse. As cybercrime grows in scale and complexity, digital signatures are increasingly being used in fraudulent activities. Forgery, identity theft, unauthorized key access, and the use of fake digital certificates have become pressing concerns. Law enforcement agencies

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 12 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

are often unprepared to deal with these challenges due to technical limitations, jurisdictional issues, and insufficient legal frameworks. These shortcomings raise important questions about the capacity of current criminal justice systems to adapt to the digital age. This paper explores the key challenges faced by criminal law enforcement in dealing with crimes involving digital signatures and proposes legal, technological, and procedural solutions to bridge the gap between innovation and regulation.

TECHNICAL CONCEPTS OF DIGITAL SIGNATURES

Definition and Underlying Technology

A digital signature is a cryptographic mechanism used to validate the authenticity and integrity of digital data, ensuring that a message or document has not been altered and confirming the identity of the signer. Unlike handwritten signatures, digital signatures employ asymmetric cryptography or public key cryptography, which uses a pair of mathematically related keys a private key and a public key.[1] The signing process involves generating a hash of the original message using a hash function. This hash is then encrypted with the signer's private key, producing the digital signature. The recipient decrypts the signature with the signer's public key and compares the resulting hash with a newly computed hash of the message. A match authenticates the sender and confirms message integrity.[2]

Public Key Infrastructure

The Public Key Infrastructure provides the framework that supports digital signatures by managing keys and digital certificates. Public Key Infrastructure comprises Certificate Authorities, Registration Authorities, digital certificates, and repositories. Certificate Authorities issue and revoke digital certificates that bind public keys to verified identities, establishing a chain of trust critical for validating signatures in a decentralized environment.[3] Public Key Infrastructure involves protocols and policies ensuring that keys are securely generated, stored, and revoked when compromised. Without robust Public Key Infrastructure, the trustworthiness of digital signatures diminishes, exposing systems to attacks such as certificate forgery or man- in-the-middle attacks.[4]

Security Properties

Digital signatures provide several key security features:

- Authentication: Verifies the signer's identity.
- Integrity: Detects any alteration to the signed data after signing.
- Non-repudiation: Prevents the signer from denying the authenticity of their signature.[5]

These features make digital signatures indispensable for secure electronic transactions, especially in sectors such as finance, government, and e-commerce.

Technical Vulnerabilities

Despite their cryptographic strength, digital signatures face potential vulnerabilities:

- Private Key Compromise: Theft or unauthorized use of the private key undermines signature security.
- Certificate Authority Breach: Compromise of a CA may allow issuance of fraudulent certificates.
- Algorithm Weaknesses: Advances in computational power or cryptanalysis can weaken hash functions or encryption algorithms used in digital signatures.[6]

These vulnerabilities can be exploited by cybercriminals to commit fraud or identity theft, posing challenges for criminal law enforcement.

LEGAL CONCEPTS OF DIGITAL SIGNATURES

Legal Recognition of Digital Signatures

Legal frameworks globally recognize digital signatures as valid and enforceable means of

executing electronic contracts and transactions. This legal acceptance ensures that digital signatures hold the same evidentiary value as handwritten signatures. For instance, the Indian Information Technology Act, 2000 provides legal recognition to digital signatures and electronic records, equating them to traditional signed documents under specific conditions.[7] Similarly, the Electronic Signatures in Global and National Commerce (ESIGN) Act, 2000 in the United States establishes the validity of electronic signatures, preventing their denial of legal effect solely because they are electronic.[8] The European Union's eIDAS Regulation sets out a legal framework for electronic identification and trust services, introducing the concept of "qualified electronic signatures," which have the highest legal status.[9]

Types of Electronic Signatures

Legal frameworks distinguish among various types of electronic signatures with differing levels of security and evidentiary value:

- Simple Electronic Signatures (SES): Basic forms such as scanned images or typed names. These are easier to implement but offer limited assurance regarding authenticity.[10]
- Advanced Electronic Signatures (AES): These are uniquely linked to the signer, capable of identifying the signer, and created with means under the signer's sole control. AES can detect data tampering.[11]
- Qualified Electronic Signatures (QES): These use a qualified certificate issued by a trusted Certification Authority and are created using secure signature creation devices. QES carry the same legal effect as handwritten signatures across the EU.[12]

Evidentiary Requirements and Challenges

For digital signatures to be admissible as evidence in court, they must satisfy certain criteria:

- Authenticity of the signer must be demonstrable.
- Integrity of the signed data must be maintained.
- The signing process must be verifiable and trustworthy.[13]

However, courts often face difficulties due to the technical complexity of digital signatures and insufficient technical expertise, especially in cases where certificate authorities are compromised or the chain of trust is broken. These issues impact the strength and admissibility of digital signatures as evidence in criminal law.[14]

Jurisdictional and Regulatory Issues

Digital signatures often operate in cross-border environments. Variations in legal recognition and standards among countries can complicate the enforcement of digital signature laws and present jurisdictional challenges for criminal investigations.[15] Harmonization efforts like the Council of Europe's Convention on Cybercrime aim to address these challenges by promoting international cooperation and uniform legal frameworks.

INTERNATIONAL FRAMEWORK ON DIGITAL SIGNATURES

United Nations and UNCITRAL Model Laws

The United Nations Commission on International Trade Law (UNCITRAL) has developed key model laws to facilitate the global acceptance of electronic commerce and digital signatures. The UNCITRAL Model Law on Electronic Commerce (1996) and the Model Law on Electronic Signatures (2001) encourage states to adopt frameworks that grant legal recognition to electronic and digital signatures, provided reliability and authenticity conditions are met.[16]

These model laws are not binding but serve as templates for national legislation, aiming to promote functional equivalence between electronic and paper-based signatures in international trade.[17]

Council of Europe - Convention on Cybercrime

The Convention on Cybercrime (Budapest

Convention), adopted by the Council of Europe in 2001, is the first international treaty to address cybercrime comprehensively, including offenses involving digital signatures, computer-related forgery, and data integrity violations.[18]

It obliges signatory states to:

- Criminalize illegal access, data interference, and system interference.
- Provide for procedural powers such as search and seizure of digital evidence.
- Cooperate internationally in investigations involving digital technologies, including the misuse of digital signatures.

This convention is especially important for cross-border enforcement and digital signature fraud, which often involve international elements.

European Union – eIDAS Regulation

The EU Regulation (EU) No. 910/2014, known as eIDAS, provides a uniform legal framework across EU Member States for electronic identification and trust services, including digital signatures. It classifies electronic signatures into three categories:

- Electronic Signature (ES)
- Advanced Electronic Signature (AES)
- Qualified Electronic Signature (QES)

QES, backed by a qualified digital certificate and a secure signature creation device, is legally equivalent to a handwritten signature under EU law.[19]

This regulation ensures mutual recognition of qualified electronic signatures across EU nations and sets technical and supervisory standards for Trust Service Providers (TSPs).

United States – ESIGN Act and UETA

In the United States, the Electronic Signatures in Global and National Commerce (ESIGN) Act of 2000 and the Uniform Electronic Transactions Act (UETA) provide the legal basis for the enforceability of electronic signatures.[20] Under these laws:

- A signature may not be denied legal effect solely because it is in electronic form.
- Consent to do business electronically is necessary.
- Signatures must be attributable to the person purported to have signed.

While not specifically using the term "digital signature," the Acts cover digital signatures under the broader term of "electronic signatures."

INDIAN LEGAL FRAMEWORK ON DIGITAL SIGNATURES INFORMATION TECHNOLOGY ACT, 2000

Legal Recognition of Digital Signatures

The Information Technology Act, 2000, is the principal legislation in India governing digital signatures and electronic transactions. Section 5 of the Act provides legal recognition to digital signatures, stating that when any law requires a signature, such requirement is satisfied if a digital signature is affixed in a prescribed manner.[21]

The Act defines a "digital signature" as the authentication of an electronic record by a subscriber using an electronic method or procedure in accordance with the provisions of Section 3.[22]

Authentication Using Asymmetric Cryptography

Section 3 of the IT Act stipulates that digital signatures must use an asymmetric cryptosystem and a hash function, which ensures the authenticity and integrity of the electronic record. The subscriber uses a private key to sign, and a public key is used for verification.[23]

This mechanism ensures that:

- The signer's identity can be verified.
- The signed document has not been altered post-signing.
- The signer cannot deny the signature

(non-repudiation).

Role of Certifying Authorities and the CCA
Certifying Authorities (CAs)

Sections 17 to 34 of the IT Act provide the legal framework for Certifying Authorities (CAs) - entities that issue Digital Signature Certificates (DSCs) to individuals and organizations after verifying their identity. These certificates serve as proof that the public key in the signature belongs to the named individual.[24] CAs must adhere to strict regulations, including maintaining secure infrastructure, revoking compromised certificates, and submitting to regular audits.

Controller of Certifying Authorities (CCA)

The Controller of Certifying Authorities (CCA), appointed under Section 17, regulates and oversees the functioning of all licensed Certifying Authorities in India. The CCA issues

guidelines, monitors compliance, and ensures that digital signatures are issued and used securely.[25] The CCA operates under the Ministry of Electronics and Information Technology (MeitY) and also maintains the Root Certifying Authority, which digitally signs the public keys of licensed CAs.

Electronic Signature (Amendment by 2008)

The Information Technology (Amendment) Act, 2008 introduced the concept of "electronic signatures" under Section 2(1) (ta), broadening the scope beyond traditional digital signatures. Section 3A allows the use of other electronic authentication techniques as prescribed, provided they are:

- Unique to the signatory.
- Capable of identifying the signatory.
- Created under the signatory's exclusive control.
- Linked to the document so that alterations invalidate the signature.[26]

This provision allowed the use of technologies such as biometric-based authentication and OTPs, increasing flexibility in digital verification.

Digital Signature Certificates (DSCs)

As per Section 35 of the IT Act, a Digital Signature Certificate is issued by a Certifying Authority upon application, confirming that the named individual holds the corresponding private key. The certificate includes:

- The public key.
- Identification details of the subscriber.
- The CA's digital signature.
- Validity period of the certificate.[27]

DSCs are now commonly used in filing income tax returns, signing government tenders, and secure banking transactions.

EVIDENTIARY VALUE AND ADMISSIBILITY

Indian Evidence Act, 1872

Section 65B of the Indian Evidence Act, 1872, inserted through the Information Technology Act, 2000, provides the legal basis for the admissibility of electronic records, including digital signatures. It stipulates that any electronic record presented as evidence must be accompanied by a Section 65B(4) certificate that confirms:

- The manner in which the electronic record was produced,
- The device used for production,
- The reliability of the source, and
- The responsibility of the person producing the certificate.[28]

Without this certificate, electronic evidence is not admissible, even if it is otherwise relevant.

Presumptions Relating to Electronic Records

Sections 85A, 85B, 85C, 88A, and 90A of the Indian Evidence Act introduce legal presumptions related to the authenticity of electronic agreements and digital signatures. For example:

- Section 85B(1) presumes the correctness of a secure digital signature unless proven otherwise.[29]

- Section 85C presumes the validity of a Digital Signature Certificate issued by a licensed CA.

EVIDENTIARY CHALLENGES IN CRIMINAL LAW ENFORCEMENT

The integration of digital signatures into modern communication and documentation has brought about unprecedented convenience, security, and legal recognition. However, in the realm of criminal law enforcement, this advancement introduces a host of complex challenges. Law enforcement agencies face significant hurdles in the investigation, admissibility, authentication, and prosecution of crimes involving digital signatures, especially as cybercrime becomes increasingly sophisticated and transnational in nature.

Technical Complexity and Lack of Expertise

Law enforcement officers often lack adequate training in handling digital evidence, particularly those involving public key infrastructure (PKI), asymmetric encryption, and hash algorithms used in digital signatures.[1] Investigators and even judges may struggle to understand how a digital signature is created, verified, or compromised. This lack of technical knowledge hampers the ability to interpret evidence accurately, leading to procedural lapses or wrongful exclusions

Non-Compliance with Section 65B

In practice, investigators frequently fail to generate or submit valid Section 65B certificates. In criminal trials, particularly those involving cyber fraud or data breaches, this oversight results in otherwise valid digital signature evidence being rendered inadmissible.

Tampering and Chain of Custody

Maintaining the integrity and chain of custody of digital evidence is critical. If a digital record is altered after being signed, or if the signing device is compromised, the signature's authenticity can be questioned. This challenge is compounded in cases where digital devices change multiple hands before reaching forensic labs.

Forged Digital Signatures and Key Misuse

While digital signatures are cryptographically secure, private keys can be stolen, leading to fraudulent signing. Proving intent, knowledge of key compromise, or unauthorized access becomes legally and technically complex, especially if the signatory denies the act.

Cross-border Investigation Hurdles

The integrity of a digitally signed document can be called into question if the chain of custody is not properly maintained. Any unauthorized alteration—even unintentional—can result in the digital signature being invalidated. Since digital evidence is easily duplicable, courts require a demonstrably secure process showing how the evidence was collected, stored, and analyzed.[30]

Burden of Proof and Rebuttal

Even though digital signatures benefit from a presumption of authenticity, the opposing party may rebut them by proving:

- The private key was compromised,
- The digital certificate had expired or was revoked at the time of signing,
- The signature creation data was not under the exclusive control of the signatory.

In such cases, forensic analysis of metadata, IP logs, access controls, and key logs become essential to establishing authenticity or forgery.

Jurisdiction and Cross-Border Investigation

Many crimes involving digital signatures span across jurisdictions, making extraterritorial enforcement highly problematic. If a digital signature is verified by a foreign certifying authority or the fraud involves servers located overseas, Indian investigators must rely on Mutual Legal Assistance Treaties (MLATs) or letters rogatory. These processes are slow, bureaucratic, and often ineffective for time-sensitive criminal cases.[31]

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 12 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Limited Forensic Capabilities

India suffers from a shortage of dedicated digital forensic labs with expertise in verifying digital signatures. Even when such labs exist, they are overburdened with pending cases, leading to delays that can compromise the quality and credibility of digital evidence. This gap affects both investigation and trial stages of criminal proceedings.

Uncooperative Private Entities

Digital signature certificates are often issued by private Certifying Authorities (CAs) under the regulation of the Controller of Certifying Authorities (CCA). In practice, these CAs may hesitate to cooperate fully with law enforcement due to data privacy concerns, lack of standard protocols, or fear of legal liabilities. This limits investigators' access to crucial verification records or audit logs maintained by CAs.[32]

Lack of Public Awareness

Victims of cyber fraud involving digital signatures often lack awareness of the legal status or security of their digital credentials. Many fail to report crimes promptly or do not preserve essential digital artifacts like certificates or timestamps. This impedes effective investigation and delays the prosecution process.

CASE LAWS

Anvar P.V. v. P.K. Basheer, (2014)

Anvar P.V., a candidate in the Kerala Legislative Assembly elections (2011), filed an election petition alleging that P.K. Basheer, his opponent, had engaged in corrupt practices, including using religious propaganda and defamatory songs to influence voters. As evidence, Anvar submitted audio CDs and transcripts of recorded speeches and songs. However, these electronic records were not accompanied by a certificate under Section 65B(4) of the Indian Evidence Act, 1872. In this landmark judgment, the Supreme Court of India held that electronic records, including those authenticated by digital signatures, must be accompanied by a certificate under Section 65B (4) of the Indian Evidence Act, 1872 to be admissible. The Court emphasized the procedural requirement of proper certification for digital evidence and overruled the earlier relaxed standard in the Navjot Sandhu case.[33]

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020)

The case involved a dispute regarding admissibility of electronic evidence in a revenue recovery proceeding. The appellant relied on electronic documents as evidence, which were submitted without the mandatory certificate under Section 65B(4) of the Indian Evidence Act, 1872. The question arose whether the documents could be admitted without the certificate, particularly in non-criminal proceedings. This decision reaffirmed the principles laid down in Anvar and further clarified that the Section 65B certificate must be submitted at the time of filing the electronic evidence. It also explained that law enforcement agencies and authorized officials must ensure compliance, especially in criminal cases involving cyber evidence or digital signatures.[34]

State (NCT of Delhi) v. Navjot Sandhu

The case involved the prosecution of Afzal Guru for his alleged role in the 2001 Indian Parliament attack. The prosecution relied heavily on electronic evidence, including telephone call records, emails, and other computer-generated documents. The defense challenged the admissibility of these electronic records, arguing that they lacked proper authentication and certification under the Indian Evidence Act. In this earlier case, the Supreme Court allowed oral evidence and traditional rules to admit electronic records, even in the absence of a Section 65B certificate. This approach was later overruled by Anvar P.V., which insisted on stricter evidentiary safeguards for digital records.[35]

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

VOLUME 5 AND ISSUE 12 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

Shafhi Mohammad v. State of Himachal Pradesh

The appellant, Shafhi Mohammad, was convicted based partly on electronic evidence such as mobile call records. The defense challenged the admissibility of such electronic records on the ground that the prosecution did **not produce a certificate under Section 65B** of the Indian Evidence Act, 1872. The trial court admitted the evidence without the certificate, but the defense argued that this violated the mandatory requirement for electronic evidence. This case temporarily **relaxed the mandatory nature** of the Section 65B certificate, holding that it may not be required if the person presenting the evidence is not in control of the device. However, this view was later overturned by the Arjun Panditrao judgment.[36]

Tata Sons Ltd. v. Greenpeace International

In this Delhi High Court case, digitally signed emails were admitted as evidence in a defamation and trademark infringement suit. The Court acknowledged the validity of digital signatures and emphasized the importance of complying with procedural requirements under the IT Act and the Evidence Act[37].

R v. Fellows and Arnold, [1997]

The defendants, Fellows and Arnold, were prosecuted for possession and distribution of child pornography. Evidence included computer records and digital images seized from their computers. The defense challenged the admissibility of these digital records on grounds related to authenticity and the proper handling of electronic evidence. A landmark UK case where computer records were admitted in a child pornography case. The Court upheld that digital evidence could be admitted if properly authenticated, thus setting early standards for computer- generated evidence in criminal trials[38]

Lorraine v. Markel American Insurance Co.,

In this U.S. case, the court issued a comprehensive ruling outlining the criteria for admitting electronic evidence, including digital signatures. The judgment emphasized five key standards: relevance, authenticity, hearsay, original writing rule, and no unfair prejudice.[39]

Sonu @ Amar v. State of Haryana

In this case, the accused (Sonu @ Amar) was convicted for offences under the Indian Penal Code. The Supreme Court held that the certificate under Section 65B is mandatory for admissibility of secondary electronic records (like CDRs). However, in this case, since the objection to admissibility was not raised at the trial stage, the Court allowed the evidence to stand[40].

R v. Governor of Brixton Prison, ex parte Levin

The High Court dismissed Levin's challenge, holding that: Cross-border cybercrimes can be subject to extradition if they have direct effects in the requesting country. There was sufficient evidence of criminal conduct under both U.K. and U.S. law (dual criminality principle). The extradition request was lawful, and extradition did not violate Levin's rights under English law.[41]

CONCLUSION

Digital signatures are a cornerstone of secure digital communication in the modern ICT-driven world. Their ability to verify identity and ensure data integrity has transformed the way digital transactions are carried out, enabling greater efficiency, transparency, and legal validity. However, as the digital ecosystem evolves, so do the threats. The misuse of digital signatures ranging from forgery and impersonation to large-scale cyber fraud poses a serious risk to both individuals and institutions. Criminal law enforcement agencies face significant obstacles in addressing these threats. The complexity of digital evidence, lack of technical expertise, cross-border jurisdictional issues, and inadequate regulatory oversight collectively hinder effective investigation and prosecution. Moreover, the fast-paced nature of technological change often outpaces the development of relevant legal frameworks, leaving gaps that can be exploited by cybercriminals. To overcome these

challenges, a multifaceted approach is required. This includes updating and harmonizing legal frameworks, enhancing international cooperation, investing in digital forensic capabilities, and providing specialized training for law enforcement and judicial officers. Only through such comprehensive efforts can the integrity of digital signatures be protected and the trust of users maintained. In conclusion, while digital signatures represent a powerful tool for securing electronic transactions, their potential for misuse demands a proactive and informed response from legal and enforcement systems. Bridging the gap between law and technology is not just desirable—it is essential for justice and security in the digital era.

REFERENCE

1. Ramaswamy, R. (2019). *Law Relating to Electronic Contracts and Digital Signatures in India*. LexisNexis.

2. Kumar, P. (2021). *Cyber Laws in India: A Commentary on the Information Technology Act, 2000*. Universal Law Publishing.

3. Subramanian, S. R. (2018). "Cyber Crime and Digital Evidence: Challenges Faced by Law Enforcement," *International Journal of Law and Management Studies*, 3(2), 142– 150.

4. Kumar, S. (2021). "Challenges in Admissibility of Electronic Evidence in India,"

International Journal of Law and Legal Studies, 9(1), 65–73.

5. Dubey, V. (2019). "Cross-Border Data Requests and MLATs: An Indian Perspective,"

National Law School of India Review, 27(1), 132–140.

6. Chander, A. (2015). "The Electronic Signature Revolution," *Georgetown Law Journal*, 103(2), 475–520.

7. UN Commission on International Trade Law (UNCITRAL). *Model Law on Electronic Commerce* (1996).

8. European Union. *eIDAS Regulation (EU) No 910/2014* on electronic identification and trust services for electronic transactions.

9. Controller of Certifying Authorities (India). https://www.cca.gov.in – official regulations, CA guidelines, and public key directories.

10. Ministry of Electronics and Information Technology (MeitY), Government of India. https://www.meity.gov.in – policy papers, notifications, and digital signature framework.

11. National Cyber Crime Rep

12. Law Commission of India, Report No. 185: *Review of the Indian Evidence Act, 1872* (2003).

13. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

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

15. *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.

16. *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.

17. *Tata Sons Ltd. v. Greenpeace International,* 178 (2011) DLT 705.

18. *R v. Fellows and Arnold*, [1997] 1 Cr App R 244 (UK).

19. *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007) (USA).

ENDNOTES

1 Whitfield Diffie & Martin E. Hellman, New Directions in Cryptography, 21 IEEE Transactions on Information Theory 644 (1976).

2 Ronald L. Rivest et al., A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Vol. 21, No. 2, 120-126 (1978).

3 Markus Jakobsson & Ari Juels, Certificate Authority Compromise and Implications for PKI, in Network and Distributed System Security Symposium (2000).

4 Clifford Neuman et al., Public-Key Infrastructure, 42 IEEE Computer 38 (2009).

5 Information Technology Laboratory, National Institute of Standards and Technology, Digital Signature Standard (DSS), FIPS PUB 186-4 (2013).

6 Mihir Bellare & Thomas Ristenpart, Advances in Cryptanalysis and Their Impact on Security, J. Cryptology 29, 507-532 (2016).

7 Information Technology Act, No. 21 of 2000, INDIA, S.S. 5, 35 (2000).

8 Electronic Signatures in Global and National Commerce Act (ESIGN), 15 U.S.C. S. 7001 (2000).

9 Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), 2014 O.J. (L 257).

10 Id. art. 3(10).

11 Id. art. 3(11).

12 Id. art. 3(12).

13 Lori Andrews, The Legal Challenges of Electronic Signatures, 22 Comput. L.J. 1 (2002).

14 K. Sharma, Cyber Forensics and Law Enforcement Challenges, 10 Int'l J. Cyber Criminology 45 (2016).

15 Council of Europe, Convention on Cybercrime, ETS No. 185, Nov. 23, 2001.

16 U.N. Comm'n on Int'l Trade Law (UNCITRAL), Model Law on Electronic Commerce with Guide to Enactment

(1996).

17 U.N. Comm'n on Int'l Trade Law (UNCITRAL), Model Law on Electronic Signatures (2001), U.N. Doc. A/56/17.

18 Council of Europe, Convention on Cybercrime, ETS No. 185, Nov. 23, 2001

19 Regulation (EU) No. 910/2014 of the European Parliament and of the Council on Electronic Identification and Trust Services (eIDAS), 2014 O.J. (L 257) 73.

20 Electronic Signatures in Global and National Commerce Act (ESIGN), 15 U.S.C. § 7001 (2000); Uniform Electronic Transactions Act (UETA), Nat'l Conf. of Comm'rs on Unif. State Laws (1999).

21 Information Technology Act, No. 21 of 2000, S. 5, INDIA.

22 Id. S. 2(1)(p).

23 Id. S. 3.

24 Id. S.S. 17–34.

25 Id. S. 17; See also: Ministry of Electronics and Information Technology, Government of India, https://www.meity.gov.in.

26 Information Technology (Amendment) Act, 2008, S. 3A.

27 IT Act, supra note 1, S. 35.

28 Indian Evidence Act, No. 1 of 1872, § 65B, INDIA (as amended by the Information Technology Act, 2000).

29 Indian Evidence Act, 1872, § 85B(1).

30 Shubham Kumar, Challenges in Admissibility of Electronic Evidence in India, 9 I.J.L. & Legal Stud. 65, 70 (2021).

31 Vivek Dubey, Cross-Border Data Requests and MLATs: An Indian Perspective, 27 Nat'l L. Sch. India Rev. 132, 136 (2019).

32 Information Technology Act, No. 21 of 2000, § 30–34 (India).

33 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).

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

35 State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India).

36Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801 (India).

37 Tata Sons Ltd. v. Greenpeace International, 178 (2011) DLT 705 (India).

38 R v. Fellows & Arnold, [1997] 1 Cr. App. R. 244 (Eng.).

39 Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007) (U.S.)

40 Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570 (India).

41 R v. Governor of Brixton Prison, ex parte Levin, [1997] EWHC Admin 1021 (UK).