E-ISSN No : 2456-5040 | Volume : 11 | Issue : 5 | May 2026

CYBER CRIME LAWS AND DIGITAL EVIDENCE: EMERGING LEGAL CHALLENGES IN INDIA

Dr. Rijwani Pinkyben Ashok kumar

Access Online

Article DOI:
10.5281/zenodo.21239530

ABSTRACT

Cyber crime has emerged as a major challenge in the digital era due to the rapid growth of internet usage, online transactions, and technological dependence. In India, increasing adoption of digital platforms, mobile banking, e-commerce, and social media has created new opportunities for economic development, but it has also led to a rise in cyber fraud, hacking, identity theft, data breaches, cyber stalking, and online harassment. This paper examines the concept and nature of cyber crime, the legal framework governing cyber offences, and the growing importance of digital evidence in investigation and prosecution. It also analyses the admissibility of electronic evidence under Indian law and the challenges faced by enforcement agencies in dealing with evolving cyber threats. The study highlights the need for stronger cyber laws, advanced forensic infrastructure, public awareness, and institutional preparedness. A balanced legal and technological approach is essential to ensure cyber security, justice delivery, and trust in the digital ecosystem.

KEYWORDS: Cyber Crime, Digital Evidence, Cyber Law, Hacking, Identity Theft, Data Breach, Online Fraud, Electronic Evidence, Cyber Security, India

1. INTRODUCTION

Cyber crime has emerged as one of the most significant legal and social challenges of the twenty-first century. With the rapid advancement of information technology, the internet has become an inseparable part of modern life, influencing communication, education, commerce, governance, entertainment, and financial transactions. While digital transformation has created immense opportunities for economic growth and social development, it has also given rise to new forms of criminal activity conducted through computers, mobile devices, and online networks. These unlawful activities, commonly referred to as cyber crimes, pose serious threats to individuals, businesses, and governments alike. In India, where digitalization has expanded at an unprecedented pace, cyber crime has become a pressing concern requiring urgent legal and institutional attention.

The term cyber crime generally refers to offences committed using computers, digital devices, communication networks, or the internet. It includes both crimes in which technology is the target and crimes in which technology is the tool used to commit traditional offences in a modern form. For example, hacking into a computer system, spreading malware, stealing confidential data, and disrupting online services are crimes where technology itself is attacked. On the other hand, online fraud, identity theft, cyber stalking, phishing scams, and digital extortion involve the use of technology as a medium for illegal gain or harassment. Cyber crime is unique because it can be committed remotely, anonymously, quickly, and across territorial boundaries, making detection and prosecution more difficult than many conventional crimes.

How to Cite:
Dr. Rijwani Pinkyben Ashok kumar (2026), Cyber Crime Laws and Digital Evidence: Emerging Legal Challenges in India, International Educational Applied Scientific & Research Journal (IEASRJ), Vol: 11, Issue: 5, 13-23

Research Paper

The concept of cyber crime has evolved alongside technological progress. In the early years of computerization, cyber offences were mostly limited to unauthorized access and basic system intrusions. However, the widespread availability of smartphones, cloud computing, artificial intelligence, social media platforms, and digital payment systems has significantly expanded the range and sophistication of cyber offences. Criminals now exploit vulnerabilities in software systems, deceive users through social engineering techniques, and use encrypted communication channels to conceal their identities. As a result, cyber crime is no longer confined to technically skilled hackers alone; organized criminal groups, financial fraudsters, insiders, and even ordinary individuals can participate in cyber offences using readily available digital tools.

The growth of internet usage in India has been extraordinary over the past decade. Affordable smartphones, declining data costs, expansion of broadband connectivity, and government initiatives promoting digital inclusion have brought millions of citizens online. Internet access has reached urban centers as well as rural areas, transforming the way people interact with markets and public institutions. Citizens increasingly rely on digital platforms for communication, education, healthcare services, entertainment, e-governance services, and employment opportunities. Social media applications have become major channels for public expression and business promotion, while online marketplaces have reshaped consumer purchasing behavior.

At the same time, digital payments and online financial transactions have grown rapidly in India. The expansion of mobile banking, Unified Payments Interface (UPI), e-wallets, internet banking, and contactless payment systems has revolutionized the financial ecosystem. Consumers can transfer funds instantly, pay utility bills, shop online, invest in securities, and manage accounts through mobile applications. Businesses of all sizes, from large corporations to small street vendors, increasingly depend on digital transactions. This shift toward a cash-light economy has improved convenience and efficiency, but it has also created new opportunities for cyber criminals to exploit unsuspecting users and vulnerable systems.

The rapid digitalization of society has been accompanied by a noticeable increase in cyber offences. Cyber fraud has become one of the most common forms of digital crime. Fraudsters frequently impersonate bank officials, customer care executives, government authorities, or trusted companies to deceive individuals into sharing passwords, one-time passwords (OTPs), card details, or personal information. Phishing emails, fake websites, malicious links, and fraudulent mobile applications are widely used to steal money or data. Many victims suffer financial losses because of a lack of digital awareness or because criminals exploit trust and urgency to manipulate them.

Hacking incidents have also become more frequent and damaging. Unauthorized access to personal accounts, corporate servers, and government databases can lead to theft of confidential information, disruption of services, or reputational harm. In some cases, attackers deploy ransomware, a form of malicious software that locks files or systems until payment is made. Such attacks can affect hospitals, educational institutions, businesses, and public agencies, causing operational paralysis and economic damage. As organizations increasingly store valuable information digitally, the incentive for cyber intrusions continues to rise.

Identity theft represents another serious concern in the digital era. Personal information such as names, addresses, identification numbers, passwords, biometric data, and banking credentials may be stolen and misused for fraudulent purposes. Criminals can open fake accounts, secure loans, conduct illegal transactions, or impersonate individuals online. In a country as digitally connected as India, misuse of personal data can have severe financial, legal, and psychological consequences for victims. The increasing use of digital KYC systems and interconnected databases makes data protection a matter of national importance.

Data breaches have further intensified concerns regarding cyber security and privacy. When organizations fail to adequately secure databases containing customer information, sensitive records may be exposed to unauthorized persons. Breaches involving financial institutions, telecom companies,

healthcare providers, educational institutions, and e-commerce platforms can affect millions of users simultaneously. Once leaked, personal data may be sold on illegal markets, used for future scams, or exploited for targeted manipulation. These incidents demonstrate that cyber crime is not merely an individual problem but a systemic risk affecting trust in the digital economy.

Online harassment and abuse have also expanded with the growth of social media and messaging platforms. Cyber stalking, trolling, defamation, circulation of obscene content, revenge pornography, threats, impersonation accounts, and hate speech have become common issues. Women, children, public figures, and vulnerable communities are often disproportionately affected. Unlike traditional harassment, online abuse can spread rapidly, remain permanently accessible, and reach large audiences within minutes. This creates significant emotional distress and raises important questions about freedom of speech, privacy, dignity, and platform accountability.

The increasing scale and complexity of cyber crime highlight the urgent need for strong cyber laws in India. Legal systems must be capable of addressing offences that involve rapidly changing technologies, anonymous actors, and cross-border networks. Existing laws need continuous updating to cover new forms of crime such as cryptocurrency fraud, artificial intelligence-enabled deception, deepfake misuse, and attacks on critical infrastructure. Effective cyber laws should clearly define offences, prescribe proportionate penalties, protect victims, safeguard privacy rights, and empower authorities to investigate crimes within constitutional limits.

Equally important is the establishment of reliable digital evidence systems. Since cyber offences are committed through electronic means, investigation and prosecution depend heavily on digital evidence such as emails, call records, IP logs, CCTV footage, metadata, chat histories, server logs, transaction records, and device contents. Such evidence must be collected, preserved, analysed, and presented in accordance with legal standards to ensure authenticity and admissibility in court. If digital evidence is mishandled, altered, or obtained unlawfully, prosecutions may fail despite the existence of wrongdoing. Therefore, trained investigators, cyber forensic laboratories, secure chain-of-custody procedures, and judicial understanding of technological issues are essential components of modern criminal justice.

2. CONCEPT AND NATURE OF CYBER CRIME

Cyber crime refers to unlawful activities that are committed through the use of computers, digital devices, communication systems, or the internet. It represents a modern form of criminal conduct in which technology either becomes the target of the offence or the means through which the offence is carried out. In the digital age, computers, smartphones, servers, online networks, and cloud systems have become central to personal, commercial, and governmental activities. As dependence on such technologies has increased, criminal behaviour has also shifted into cyberspace, creating new challenges for law enforcement agencies and legal systems. In India, where digital connectivity is rapidly expanding, cyber crime has become an important issue affecting economic security, privacy, and public trust.

The concept of cyber crime is broader than traditional crime because it includes offences that may not involve physical presence or direct personal contact between the offender and victim. A person may commit a cyber offence while sitting in one city or even another country, targeting victims located elsewhere. Through anonymous accounts, hidden networks, encryption tools, and virtual private systems, offenders can conceal their identities and operate across multiple jurisdictions. This borderless character distinguishes cyber crime from many conventional offences and makes investigation, prosecution, and punishment more complex.

Cyber crime can generally be understood in two major ways. First, there are offences where the computer system, network, or digital infrastructure itself is the target. These include hacking, unauthorized access, denial-of-service attacks, malware distribution, ransomware attacks, website defacement, and destruction or alteration of electronic data. In such cases, the attacker seeks to damage, disrupt, control, or misuse technological systems. Second, there are offences where technology is used as a tool to commit

traditional crimes in a new form. These include cheating, fraud, identity theft, extortion, stalking, defamation, forgery, obscenity, and financial scams conducted through digital platforms. The internet has therefore become both a new crime scene and a new criminal instrument.

The nature of cyber crime is dynamic and continuously evolving. Unlike many conventional crimes that rely on physical force or direct confrontation, cyber offences often depend on technical skill, deception, manipulation, and exploitation of system weaknesses. Criminals frequently use social engineering methods to trick users into revealing passwords, bank details, or confidential information. They may send fake messages, create fraudulent websites, impersonate trusted organizations, or install malicious software on devices. This means that cyber crime is not limited to sophisticated programming attacks; many offences succeed through psychological manipulation of users rather than complex coding.

Another important feature of cyber crime is speed and scale. A traditional theft may affect one person or one place at a time, whereas a cyber attack can target thousands or even millions of users simultaneously. A phishing campaign can send fraudulent messages to countless individuals within seconds. A data breach can expose the personal information of millions of customers. Malware can spread globally through interconnected networks in a short period. Because of this scalability, cyber crime can cause extensive financial losses, reputational damage, and social disruption in a very limited period.

Cyber crime is also characterized by anonymity and difficulty of attribution. Offenders often use false identities, proxy servers, encrypted channels, cryptocurrency payments, and stolen credentials to avoid detection. Determining the real person behind an online attack may require technical tracing, digital forensics, cooperation from service providers, and international legal assistance. In many cases, criminals exploit the fact that legal procedures are slower than technological developments. This creates serious challenges for police authorities, investigators, and courts in India and across the world.

The financial motive is one of the most common drivers of cyber crime. Many offences are committed to obtain money through fraud, extortion, theft of banking credentials, unauthorized fund transfers, or sale of stolen data. Online banking scams, credit card fraud, fake investment schemes, and ransomware demands illustrate how criminals exploit digital systems for profit. However, financial gain is not the only motive. Some cyber crimes are committed for revenge, political objectives, espionage, ideological reasons, harassment, or mere curiosity. Insider attacks by disgruntled employees and cyber espionage against corporations or governments demonstrate the diversity of motives involved.

Cyber crime affects a wide range of victims. Individuals may lose savings, privacy, identity, or emotional well-being. Businesses may suffer operational disruption, loss of confidential data, legal liability, and reputational harm. Governments may face threats to public infrastructure, security systems, and citizen databases. Educational institutions, hospitals, banks, and small enterprises are equally vulnerable. Since digital technology is integrated into everyday life, cyber crime is no longer limited to specialized sectors; it has become a general societal risk.

The intangible nature of cyberspace also influences the legal treatment of cyber crime. In conventional crimes, physical evidence such as weapons, documents, fingerprints, or stolen goods may be available. In cyber offences, evidence is often electronic in nature, including IP logs, emails, chat records, metadata, device contents, transaction histories, and server records. Such evidence can be altered, deleted, encrypted, or stored across multiple jurisdictions. Therefore, successful prosecution depends on proper collection, preservation, and authentication of digital evidence.

In India, the nature of cyber crime has become more significant due to increasing internet penetration, digital payments, e-commerce growth, and widespread use of smartphones. As more citizens rely on online platforms for banking, education, employment, and communication, opportunities for cyber offenders also expand. Fraudulent customer care scams, fake loan apps, identity theft, social media abuse, and hacking incidents have become common

examples of modern cyber offences affecting everyday users.

3. LEGAL FRAMEWORK GOVERNING CYBER CRIME IN INDIA

The rapid expansion of digital technology, internet connectivity, electronic commerce, and online financial transactions has made cyber security a matter of national importance in India. As cyber offences such as hacking, identity theft, phishing, data theft, online fraud, cyber stalking, and digital extortion continue to rise, a strong legal framework is essential to regulate conduct in cyberspace and ensure protection of citizens, businesses, and public institutions. Since cyber crime often involves invisible actions, cross-border networks, and rapidly changing methods, traditional criminal laws alone are insufficient to address these modern offences. Therefore, India has developed a combination of special legislation, general criminal law, evidentiary rules, and regulatory mechanisms to combat cyber crime.

The legal framework governing cyber crime in India is not confined to a single statute. It consists of multiple laws working together to address various aspects of cyber offences, electronic transactions, privacy concerns, data protection, and prosecution procedures. The most significant legislation in this field is the Information Technology Act, 2000, which was enacted to provide legal recognition to electronic records and digital signatures while also creating specific offences related to misuse of computer resources. Over time, amendments and supplementary laws have broadened the regulatory structure to meet evolving technological challenges.

The Information Technology Act, 2000 is regarded as the cornerstone of cyber law in India. It was introduced to facilitate e-commerce, electronic governance, and digital communication, but it also contains penal provisions dealing with cyber offences. The Act defines key terms such as computer, computer network, data, intermediary, and electronic record, thereby creating a legal basis for regulating online activities. It criminalizes unauthorized access to computer systems, downloading or copying data without permission, introduction of viruses or malicious code, damage to computer networks, denial of access to authorized users, and disruption of services. The Act also provides for compensation in cases where wrongful loss or damage is caused through misuse of computer resources.

Several important offences are specifically recognized under the Information Technology Act, 2000. Identity theft through misuse of passwords, digital signatures, or unique identification credentials is punishable. Cheating by personation using computer resources, including online impersonation scams, is also covered. Publishing or transmitting obscene or sexually explicit material in electronic form is prohibited. Violations involving privacy, such as capturing or transmitting images of private areas without consent, attract penal consequences. Cyber terrorism, attacks on critical information infrastructure, and unauthorized access threatening national security are treated with particular seriousness. Through these provisions, the law recognizes that cyber crime can affect both personal rights and national interests.

Another important component of the cyber crime framework in India is general criminal law. Many cyber offences are modern forms of traditional crimes such as cheating, forgery, criminal intimidation, defamation, extortion, breach of trust, and obscenity. These offences may be prosecuted under the Bharatiya Nyaya Sanhita, 2023, which replaced the earlier Indian Penal Code. For example, online financial scams may amount to cheating, fake documents created digitally may amount to forgery, threats sent through electronic communication may constitute criminal intimidation, and defamatory statements posted online may attract legal liability. Thus, special cyber legislation and general criminal law often operate together.

Procedural law also plays a vital role in the enforcement of cyber crime legislation. Investigation, arrest, search, seizure, and trial processes are governed by criminal procedure statutes, particularly the Bharatiya Nagarik Suraksha Sanhita, 2023. Cyber investigations may require seizure of computers, mobile devices, storage media, server records, and account information. Authorities must follow lawful procedures while collecting evidence to ensure that prosecutions are valid and constitutional safeguards are respected. Since cyber offences often involve

digital evidence, procedural compliance is critical.

The law of evidence is equally significant in cyber crime cases. Electronic records such as emails, chat logs, CCTV footage, metadata, transaction records, and device contents frequently become central evidence in prosecutions. Their admissibility is governed by the Bharatiya Sakshya Adhiniyam, 2023, which replaced the earlier Indian Evidence Act. The law recognizes electronic records as evidence subject to prescribed standards of authenticity and certification. Courts require assurance that digital material has not been tampered with and that it originates from reliable sources. Therefore, digital forensics and chain-of-custody procedures are crucial in cyber crime litigation.

Data protection and privacy regulation have also become increasingly important within the cyber legal framework of India. As personal data is collected and processed by businesses, digital platforms, and public authorities, misuse or unauthorized disclosure of such information may facilitate cyber crime. The Digital Personal Data Protection Act, 2023 establishes obligations relating to lawful processing of personal data, user consent, security safeguards, and grievance mechanisms. While primarily a privacy statute, it indirectly supports cyber security by encouraging better data handling practices and accountability.

Financial cyber fraud is another major concern addressed through sectoral regulations. Reserve Bank of India guidelines on digital payments, banking security, KYC norms, fraud reporting, and customer protection are relevant in combating unauthorized transactions and phishing scams. Banks, payment service providers, and fintech entities are expected to implement security controls, fraud detection systems, and grievance redressal procedures. Regulatory oversight helps strengthen trust in the digital economy.

Intermediary regulation forms an additional part of the cyber legal framework. Social media platforms, messaging services, hosting providers, and online marketplaces play a major role in the digital ecosystem. Laws and rules governing intermediaries impose duties regarding due diligence, grievance redressal, cooperation with lawful authorities, and removal of unlawful content under specified conditions. This becomes particularly relevant in matters involving online harassment, misinformation, fake accounts, intellectual property infringement, and circulation of illegal material.

Despite the presence of multiple laws, the legal framework governing cyber crime in India faces several challenges. Technology evolves faster than legislation, creating gaps in legal coverage. Jurisdictional difficulties arise when offenders operate from foreign countries. Investigative agencies often require advanced technical expertise and better forensic infrastructure. Public awareness regarding cyber rights and responsibilities remains uneven. Questions concerning privacy, surveillance, freedom of expression, and platform liability also require careful constitutional balancing.

Judicial interpretation has played an important role in shaping cyber law in India. Courts have clarified issues relating to free speech, intermediary liability, electronic evidence, privacy rights, and misuse of statutory provisions. Landmark decisions have reinforced the principle that digital governance must remain consistent with constitutional guarantees while still enabling effective control of cyber crime.

4. DIGITAL EVIDENCE: MEANING AND IMPORTANCE

Digital evidence has become one of the most significant components of the modern justice system in the age of information technology. As communication, commerce, banking, governance, and social interaction increasingly take place through electronic platforms, traces of human activity are regularly created and stored in digital form. These electronic traces often become valuable sources of proof in civil disputes, criminal investigations, regulatory proceedings, and administrative inquiries. In India, where digital transactions and internet usage have expanded rapidly, digital evidence now plays a central role in addressing cyber crime as well as many traditional offences committed through technological means.

Digital evidence may be understood as any information of probative value that is stored, transmitted, generated, or received in electronic form

and that can be used in legal proceedings. It includes data contained in computers, mobile phones, tablets, servers, cloud systems, storage devices, surveillance systems, and communication networks. Unlike conventional evidence such as paper documents or physical objects, digital evidence exists in electronic formats and may require specialized tools and technical expertise for retrieval, preservation, and interpretation. It can reveal actions, identities, locations, communications, timelines, financial transactions, and patterns of behaviour relevant to a legal dispute or criminal act.

The concept of digital evidence is broad and continuously evolving because technology itself is constantly changing. Earlier forms of evidence were often limited to emails, hard drive files, and computer records. Today, digital evidence extends to social media posts, instant messaging records, GPS location data, biometric logs, CCTV recordings, metadata, browser history, online payment records, cloud backups, smart device data, and blockchain transaction histories. As digital ecosystems expand, nearly every electronic interaction may potentially create evidentiary material.

One of the most common sources of digital evidence is personal electronic devices such as smartphones and laptops. Mobile phones may contain call records, contact lists, text messages, emails, photographs, videos, application data, browsing history, payment logs, and geolocation records. Laptops and desktop computers may store documents, spreadsheets, deleted files, login records, software activity, and internet search histories. In many criminal cases, these devices help investigators reconstruct events, establish communication links, and determine intent.

Communication records form another vital category of digital evidence. Emails, instant messages, voice-over-internet calls, chat histories, and social media interactions can be crucial in cases involving fraud, conspiracy, threats, harassment, defamation, stalking, or contractual disputes. Messages exchanged through digital platforms may reveal motive, planning, consent, deception, or unlawful coordination. Even when messages are deleted, forensic recovery methods may sometimes retrieve remnants or associated metadata.

Financial and transactional data also carry major evidentiary value. Online banking records, Unified Payments Interface (UPI) transactions, credit card logs, e-wallet activity, e-commerce purchase histories, and cryptocurrency transfers may help trace fraud, money laundering, unauthorized transactions, or illicit gains. In India, where digital payments have become deeply integrated into everyday life, such records are increasingly important in investigations of cyber fraud and economic offences.

Surveillance and monitoring systems contribute another important category of digital evidence. CCTV footage, access control logs, biometric attendance records, vehicle tracking systems, and security camera recordings may establish presence, movement, timing, or identity. In both public and private spaces, these systems generate continuous electronic records that may corroborate witness testimony or contradict false claims. Video evidence has become especially useful in crimes involving theft, trespass, assault, and unauthorized access.

Digital evidence is particularly important in cyber crime investigations because the offence itself often occurs through electronic systems. Crimes such as hacking, phishing, identity theft, ransomware attacks, data breaches, online cheating, and cyber stalking may leave little or no traditional physical evidence. Instead, proof is found in server logs, IP addresses, access timestamps, malicious code, email headers, login credentials, transaction trails, and communication histories. Without digital evidence, many cyber offences would be difficult to detect or prove in court.

The importance of digital evidence also extends beyond cyber crime. Traditional offences such as murder, kidnapping, corruption, domestic violence, extortion, and organized crime increasingly involve digital elements. Mobile location data may place a suspect near a crime scene. Search history may indicate planning. Messages may reveal threats or conspiracy. Photographs or videos may document unlawful acts. Thus, even conventional crimes now frequently depend on electronic evidence for successful investigation and prosecution.

Another major value of digital evidence lies in its ability to establish timelines and patterns. Metadata—

data about data—can reveal when a file was created, modified, transmitted, or accessed. Login histories may show repeated unauthorized access attempts. GPS records may indicate movement over time. Transaction logs may expose recurring fraud schemes. Such patterns often provide objective and chronological insights that human memory alone cannot reliably supply.

However, the usefulness of digital evidence depends heavily on authenticity and integrity. Electronic data can be altered, deleted, encrypted, copied, or fabricated more easily than many physical forms of evidence. Therefore, legal systems require careful procedures for seizure, preservation, imaging, analysis, and presentation of digital material. Investigators must maintain a proper chain of custody to show that evidence remained secure and untampered. In India, admissibility of electronic records is governed by the Bharatiya Sakshya Adhiniyam, 2023, which recognizes electronic records subject to prescribed legal standards.

Digital forensics has become essential because of the increasing role of electronic evidence. Forensic specialists use scientific methods and specialized software to recover deleted files, analyse device contents, trace network activity, identify malware behaviour, and authenticate records. Their expertise helps courts understand complex technical material and determine whether evidence is reliable. As technology becomes more sophisticated, trained forensic professionals are indispensable to the justice process.

Despite its advantages, digital evidence also raises concerns regarding privacy, surveillance, and misuse. Excessive access to personal devices or communications may interfere with fundamental rights if not conducted lawfully. Unauthorized leaks of seized data may cause further harm to individuals. Therefore, the collection and use of digital evidence must balance investigative necessity with constitutional safeguards, due process, and data protection principles.

5. LEGAL ADMISSIBILITY OF DIGITAL EVIDENCE IN INDIA

The rapid growth of technology and digital communication has transformed the nature of evidence presented before courts. In the modern era, a large part of human interaction takes place through mobile phones, computers, email systems, online banking platforms, social media networks, surveillance devices, and cloud storage services. As a result, disputes and criminal investigations increasingly involve electronic records rather than only traditional documentary or oral evidence. Messages, emails, call records, CCTV footage, transaction logs, metadata, photographs, and digital files are now frequently relied upon in legal proceedings. Consequently, the legal admissibility of digital evidence has become a crucial aspect of the justice system in India.

Digital evidence refers to information of evidentiary value that is stored, generated, transmitted, or received in electronic form. Unlike physical evidence, electronic records are intangible and can be copied, modified, deleted, encrypted, or manipulated with relative ease. Because of this nature, courts must ensure that such evidence is genuine, relevant, and reliable before accepting it. Legal rules governing admissibility therefore seek to strike a balance between recognizing modern forms of evidence and protecting the fairness of judicial proceedings.

In India, the admissibility of digital evidence is primarily governed by the Bharatiya Sakshya Adhiniyam, 2023, which replaced the earlier Indian Evidence Act, 1872. The law formally recognizes electronic records as a valid category of evidence and places them on a legal footing comparable to traditional documentary evidence, subject to prescribed safeguards. This recognition is essential because in many contemporary cases, especially cyber crime, commercial disputes, and financial fraud matters, electronic records may constitute the most important proof available.

Electronic records may include emails, text messages, WhatsApp chats, social media posts, computer files, digital photographs, CCTV recordings, audio clips, server logs, online transaction histories, GPS data, and information stored in cloud systems. Courts may

examine such material when it is relevant to facts in issue. However, relevance alone is not sufficient. The party relying upon digital evidence must also satisfy legal requirements relating to authenticity, source, integrity, and lawful production.

One of the most significant principles governing digital evidence in India is the requirement of certification for electronic records produced from a device or system. Where a copy of an electronic record is tendered in evidence, it must generally be accompanied by a certificate confirming the manner in which the record was produced, the particulars of the device involved, and that the output accurately represents the original data maintained in the ordinary course of activities. This certificate serves as an assurance of reliability and helps reduce the risk of fabricated or altered records.

The rationale behind certification lies in the special nature of electronic data. A printed email, screenshot, pen drive copy, or transferred video file is often only a reproduction of information originally stored elsewhere. Since digital content can be easily edited or manipulated, courts require proof that the copy presented truly reflects the original electronic record. Without such safeguards, the possibility of false evidence would significantly increase. Certification therefore plays a central role in ensuring evidentiary trustworthiness.

Judicial decisions in India have strongly shaped the law relating to digital evidence. The Anvar P.V. v. P.K. Basheer decision clarified that compliance with statutory certification requirements is generally mandatory when relying on secondary electronic evidence. Later decisions, including Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, reaffirmed the importance of proper certification and explained procedural aspects concerning production of electronic records. These judgments significantly influenced how trial courts treat digital material.

Original electronic devices may also be relevant in certain cases. If the actual device containing the data, such as a mobile phone, laptop, DVR system, or server, is produced and examined, evidentiary issues may differ from cases involving copied outputs. Even then, courts may require proof linking the device to the relevant person, establishing continuity of possession, and demonstrating that the contents were not tampered with. Thus, production of the original device does not automatically eliminate all authenticity concerns.

The concept of chain of custody is extremely important in determining admissibility and evidentiary weight. Chain of custody refers to the documented history of seizure, handling, storage, transfer, and examination of electronic material from the time it is collected until it is produced before the court. If a mobile phone, hard drive, or CCTV storage unit passes through multiple hands without proper documentation, doubts may arise regarding alteration or contamination. A secure and well-recorded chain of custody strengthens confidence in the evidence.

Digital forensic examination often assists courts in evaluating electronic evidence. Experts may recover deleted files, examine metadata, verify timestamps, trace IP logs, authenticate recordings, detect editing, or analyze malware. Their reports and testimony help judges understand technical issues beyond ordinary knowledge. In complex cyber crime cases, expert evidence can be decisive in proving whether data was manipulated or whether a device was used in the commission of an offence.

The admissibility of digital evidence also depends on relevance and legality of collection. Even authentic records may be challenged if they are unrelated to the dispute or obtained in violation of procedural safeguards. Unauthorized interception, unlawful hacking, or improper seizure may raise constitutional and statutory objections. Courts must balance the need for truth-finding with privacy rights, due process, and fairness to the accused.

Screenshots, chat messages, and social media posts have become common forms of evidence in civil and criminal disputes. However, these forms are particularly vulnerable to fabrication through editing tools and fake accounts. Therefore, courts generally prefer corroboration through metadata, service provider records, device extraction reports, witness testimony, or certification rather than relying solely on bare screenshots. The evidentiary value of such

material depends on surrounding circumstances and proof of genuineness.

In commercial litigation, digital evidence is equally significant. Contracts concluded through email, electronic invoices, online purchase records, digital signatures, accounting software data, and corporate communication logs may determine rights and liabilities between parties. As businesses increasingly operate through digital systems, electronic evidence has become central to modern commerce and dispute resolution.

Despite legal recognition, practical challenges remain in India. Many investigating agencies require greater technical training. Delays in forensic examination can slow trials. Data stored on foreign servers may be difficult to obtain. Rapidly evolving technologies such as encrypted messaging, disappearing messages, artificial intelligence-generated content, and deepfakes create fresh admissibility concerns. Courts must continuously adapt legal principles to these emerging realities.

6. CONCLUSION

Cyber crime has emerged as one of the most serious legal and technological challenges of the contemporary era. The rapid expansion of internet connectivity, digital communication, e-commerce platforms, online banking, and electronic governance has transformed the social and economic landscape of India. While these developments have created immense opportunities for growth, efficiency, and inclusion, they have also exposed individuals, businesses, and public institutions to new forms of criminal activity. Cyber fraud, hacking, identity theft, ransomware attacks, online harassment, data breaches, and misuse of personal information have demonstrated that technological progress must be accompanied by strong legal safeguards and effective enforcement systems.

The study of cyber crime laws shows that India has developed an important legal foundation through the Information Technology Act, 2000, supported by the Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023. Together, these laws seek to regulate cyber conduct, punish offenders, protect victims, and provide procedural mechanisms for investigation and trial. However, the constantly evolving nature of technology means that legal systems must remain adaptive and responsive to new threats such as artificial intelligence-enabled fraud, deepfakes, cryptocurrency crimes, and attacks on critical digital infrastructure.

Digital evidence has become the backbone of cyber crime investigation and prosecution. Emails, call records, CCTV footage, chat messages, server logs, metadata, transaction records, and device data frequently provide the most reliable proof in modern cases. The legal admissibility of such evidence depends upon authenticity, proper certification, lawful collection, and secure chain-of-custody procedures. Without robust digital forensic capabilities and trained investigators, even strong substantive laws may fail in practical enforcement.

At the same time, the response to cyber crime cannot depend solely on legislation. Public awareness, cyber hygiene, institutional preparedness, timely reporting mechanisms, and cooperation between government agencies, private platforms, banks, and international authorities are equally necessary. Citizens must be educated about phishing scams, fraudulent links, identity theft, privacy protection, and safe digital practices. Organizations must strengthen cybersecurity frameworks and data governance standards.

REFERENCES

1. Desai, Niral. "Electronic Records as Evidence: A Study under the Indian Evidence Regime." Law Review Journal, vol. 10, no. 2, 2020, pp. 121-136.
2. Iyer, Sneha, and Rahul Menon. "Role of Forensic Science in Cyber Crime Investigation." Journal of Forensic and Legal Studies, vol. 3, no. 1, 2023, pp. 15-28.
3. Kumar, Sandeep. "Legal Framework for Cyber Security in India." Journal of Contemporary Legal Issues, vol. 6, no. 3, 2020, pp. 78-91.
4. Mehta, Arjun. "Cyber Stalking and Online Harassment: Legal Remedies in India." Indian Journal of Criminal Law, vol. 9, no. 4, 2021, pp. 95-108.
5. Nair, Deepa. "Emerging Trends in Cyber Law Reforms in India." Journal of Legal Innovation, vol. 2, no. 1, 2024, pp. 10-24.
6. Patel, Rakesh, and Meera Joshi. "Digital Evidence and Its Admissibility under Indian Law." Indian Journal of Legal Studies, vol. 8, no. 1, 2021, pp. 45-59.
7. Shah, Priya. "Cyber Fraud and Online Financial Crimes

in India." International Journal of Research in Law and Economics, vol. 4, no. 2, 2023, pp. 33-47.
8. Singh, Ajay, and Neha Sharma. "Cyber Crime in India: Challenges and Preventive Measures." International Journal of Law Management & Humanities, vol. 5, no. 2, 2022, pp. 112-120.
9. Trivedi, Kunal. "Phishing Attacks and Consumer Protection in Digital Banking." Asian Journal of Legal Research, vol. 5, no. 3, 2022, pp. 84-97.
10. Verma, Rohit, and Kavita Rao. "Identity Theft and Data Protection Laws in India." Journal of Information Law and Policy, vol. 7, no. 1, 2022, pp. 60-74.