Nanotechnology Perceptions
ISSN 1660-6795
www.nano-*ntp.com*

The Role Of Digital Forensics And Cyber Crime Provisions In India's New Criminal Laws

Chandan Kumar Singh[1] , Dr. Arunanshu Dubey[2]

[1]Research Scholar, ILSR, GLA University, Mathura, India.
[2](Ph.D. Supervisor) & Asst. Professor, Institute of Legal Studies & Research, GLA University, Mathura, India.

Reflecting modern requirements, new criminal law reforms in India include the Bhartiya Nyay Sanhita (BNS), the Bhartiya Nagarik Suraksha Sanhita (BNSS), and the Bhartiya Sakshya Adhiniyam (BSA) and are intended to respond to such modern challenges as cybercrime and the growing importance of digital evidence. Digital forensics has been a crucial component of criminal investigations as it provides information concerning cyber-crime comprising of hacking, data fraud, and any other unlawful utilization of digital media. The BNS forms a basis of how such offenses are classified while the BNSS features working and implementation procedures in dealing with cybercriminal conduct. The BSA, that concentrates evidence aspects, provides provisions for the admissibility of digital evidence, as the global conventions. In combination, these laws improve the landscape of cybercrime fighting in India and offer improved protection to physical persons in the information environment. This paper discusses the need for specialized tools and professionals in digital forensics to improve investigation and prosecution efficiency. It emphasizes the importance of a strong legal framework in India to reduce and overcome cyber crime complexity. The study uses a qualitative legal framework analysis of the recently enacted BNS, BNSS, and BSA (2023) and considers official legislative texts, legal commentaries, and scholarly articles from the European Union. The aim is to enhance the efficiency of digital forensics operations within the legal framework.

KEYWORDS: Digital Forensics, Cybercrime, BNS, BNSS, BSA

INTRODUCTION

On July 1, 2024, India's criminal justice system experienced a substantial overhaul with the enactment of three new laws:

(a) the "Bharatiya Nyaya Sanhita, 2023" (BNS), which supplanted the Indian Penal Code, 1860;
(b) the "Bharatiya Nagarik Suraksha Sanhita, 2023" (BNSS), which supplanted the Code of Criminal Procedure, 1973; and
(c) the "Bharatiya Sakshya Adhiniyam, 2023" (BSA), which supplanted the place of the Indian Evidence Act, 1872.

The IPC, 1860, the CrPC, 1973, and the Indian Evidence Act, 1872 (collectively referred to as the "Old Criminal Laws") will continue to govern any offences committed until midnight on June 30, 2024, as intended by the aforementioned legislations. Therefore, the Old Criminal

Laws will continue to be relevant for a number of years until all ongoing processes, including investigations, enquiries, trials, appeals, and associated actions, come to a close.

The Old Criminal Laws, originating in 1860, represent a pivotal time in India's criminal justice system. The new criminal laws have included measures designed to address the intricacies of the digital era and discourage offenses that have proliferated in the internet age. These laws recognized the expanding digital environment and included provisions to more effectively address the rising incidence of cybercrime in India. The BNS does not define cybercrime, but it encompasses technology-related offences such as hacking, phishing, and cyberstalking.

India's legal framework is seeing a significant transition with the implementation of the BNS, BNSS, and BSA. These new laws seek to modernize the criminal justice system by enhancing its effectiveness, efficiency, and accessibility. Utilizing technical breakthroughs, the new regulations aim to optimize judicial operations and enhance citizen protection, indicating a notable transition toward a more equitable legal system suited to the digital era.

One noticeable aspect of these modifications is the emphasis on digital forensics. The importance of digital forensic evidence has grown in recent years due to the increasing sophistication of both technology and threats. The new law emphasises the use of audiovisual technology to enhance police investigations at crime scenes. Section 105 of the BNSS mandates the recording of searches and seizures using audiovisual technologies. Each time police officers search a building or seize an item, they must now capture the audio and video footage. Police officers must promptly notify legal authorities of the recording and seizure list. The goal of this effort is to make sure that police operations are transparent and accountable.

In order to improve forensic evidence collection and application, the BNSS employs a number of crucial procedures. **Section 176(3)** mandates the collection of forensic evidence at crime scenes for crimes punishable by seven years or more in jail. According to **Section 176(1)**, a female police officer must interview a rape victim at the victim's home or another designated location while a parent, guardian, or social worker is present. It is also possible to use audiovisual tools to record this proof. **Section 180(3)**

grants police personnel the authority to record witness evidence using audiovisual technologies. **Section 54** permits the use of audiovisual technology to capture test identifier comments during identification parades in cases where the identifier has a mental or physical disability.

Sections 265 and 266 provide for the use of audiovisual technology to examine witnesses in warrant proceedings at locations specified by the state. Section 308 authorizes the use of technical tools, such as audio-video conferencing, to examine the accused. A magisterial order may now authorize the collection of a wider variety of forensic evidence, including voice samples (such as fingerprints, signatures, and handwriting), according to Section 349.

We anticipate many benefits from the implementation of these regulations. The BNSS encourages comprehensive investigations and convictions of cybercrimes by providing a legal basis for gathering and using digital forensic data. The use of digital forensic evidence aids law

enforcement in their investigations by reducing the time and resources needed. Digital evidence has a better chance of being admissible in court if there are clear rules on the chain of custody. The new laws do, however, bring their own set of difficulties. We need to educate the public, law enforcement, and legal professionals about digital forensics and the BNSS regulations. The successful implementation of the BNSS depends on the establishment of sufficient digital forensic laboratories and the employment of qualified workers and specialists. It is still quite difficult to find an adequate method of research while simultaneously safeguarding individuals' privacy and sensitive information.

When it comes to digital forensics, the BNSS is a huge step forward for India's judicial system. Various areas require further work to fully realise the advantages. Everyone, from advocates to members of the public and law enforcement, must have a better grasp of digital forensics and its function within the judicial system. To encourage innovation, research, and skill development in digital forensics, there must be better collaboration between academic institutions, industry, and law enforcement. To effectively collect evidence and bring those guilty to court, effective international collaboration is necessary, given the worldwide scale of cybercrime. Digital forensics is essential in contemporary justice and law enforcement; India can ensure this by fixing these problems. The BNSS represents a progressive approach to criminal justice, positioning India at the forefront of technology integration with judicial processes and law enforcement.

DIGITAL TRANSFORMATION IN THE LIGHT OF NEW CRIMINAL LAWS

The primary motivation for the revision, given the 1860 enactment of the original Indian Penal Code, was to replace archaic terminology with contemporary equivalents. Certain substitutions pertain to contemporary sensibilities, such as the replacement of the phrase "idiot." In certain instances, using contemporary vocabulary may prioritize aesthetics above content.

Section 124A of the former Indian Penal Code defined the crime of "sedition". Despite its removal, **Section 152** of the new law bears a marked similarity. Notably, the inclusion of 'electronic communication' acknowledges the use of contemporary channels or methods by individuals who "excite... or encourage separatist sentiments." The explicit inclusion of electronic communication, in conjunction with the recommendations outlined in the new Telecommunications Act of 2023, raises issues around online accountability and privacy.

According to the Telecommunications Act, internet communication service providers must "intercept, detain, disclose, or suspend any message," even if this necessitates violating the end-to-end encryption standards established for user privacy. This prompts inquiries about the degree of data security and privacy afforded to users while also indicating a significant shift in the operational practices of communication service providers moving forward.

Penalising Cybercrimes and False Information

Section 111 categorises 'cybercrime' as a kind of 'organised crime', signalling that online offences would be rigorously enforced. Section 197(d) of the BNS imposes penalties for the fabrication and dissemination of 'false information'. The meanings of these offences are broadly articulated, and it would be more legally tenable to assign exact definitions to them. The suitability of certain social media and e-commerce platforms for this formulation remains

ambiguous, as does the degree of responsibility to which these platforms may be exposed. Online platforms may need to revise their User Agreements, Terms and Conditions, and Community Guidelines, as well as modify their monitoring systems, to safeguard against responsibility for any harmful or unlawful conduct by its users.

BHARATIYA NAGARIK SURAKSHA SANHITA (BNSS) ACT NO. 46 OF 2023

Inspection and Seizure of Electronic Devices

The New Criminal Procedure Code augments the authorities granted to law enforcement during investigations. It permits the confiscation of any electronic device or record that is 'likely' to harbour digital evidence, and anyone other than the accused may also be compelled to provide such materials. A police officer may search and take an individual's property without written authorisation if there are reasonable reasons to assume that the property cannot be retrieved without excessive delay.

Indian courts have previously reasoned that the "right against self-incrimination is confined to information derived from personal knowledge." The increased authority granted to law enforcement may significantly impact investigations involving organisations or enterprises, where the likelihood of seizing electronic devices is much higher. This heightens the risk that local Indian offices of multinational corporations will incur, even when the primary business operations are conducted elsewhere. This may affect corporate operations, confidentiality, and reputation. Organisations may need to enhance their digital security measures and legal compliance plans to address these concerns.

Witness Protection Scheme

Section 398 of the new procedural code mandates that each state government establish a witness protection program to ensure the safety of witnesses. Although acknowledging the need for a 'Protection Scheme', the law does not specify its applicability to corporate whistleblowers, given that SEBI legislation concerning whistleblowing is narrowly focused on insider trading alone.

Viewed from that standpoint, the recent criminal legislation represents a failed chance to enshrine rights for whistleblowers, a provision present in all contemporary economies. It is noteworthy that while the Whistle Blowers Protection Act, 2014 was enacted by the Parliament of India in 2014, it has yet to be registered and remains unenforceable as law.

"BHARATIYA SAKSHYA ADHINIYAM, NO. 47 OF 2023"

Use of Electronic Evidence

Digital or electronic records now have the same "legal effect, validity, and enforceability" as physical documents, according to the New Evidence Code. Electronic communications are likewise considered documents as they include data saved, recorded, or replicated in a communications device's memory. It seems from the wording that digital recordings may be used as main evidence.

Not all procedural hurdles have been eliminated, even if electronic evidence is permitted. For digital evidence derived from computer output to be credible, Section 63 of the code sets requirements on its validity. This implies that there are still extremely specific requirements that must be met in order for digital records to be admissible, even if certification is not required for all digital records. According to **section 63(4), A** certificate is only necessary for digitally filed statements. In contrast, all electronic records were previously required to get a certificate under section 65B in order to be admissible under the Indian Evidence Act.

- **Data and the Right Against Self-Incrimination** Technological advancements under the new criminal legislation have consistently influenced the right to privacy. Broad, indiscriminate data seizures, without adequate checks on relevance or proportionality, conflict with constitutional safeguards against self-incrimination and violations of privacy. Therefore, it is essential to implement strict procedural and regulatory frameworks that restrict how long data can be accessed and the duration for which devices can be held by authorities. This also raises concerns for businesses in India, highlighting the urgent need for clear guidelines on how companies manage and store employee and user data, given its broader implications.
- **Privacy and Protection of Personal Information.** With greater access to personal data by the State comes a heightened duty to safeguard it. When the police hold electronic devices or records, the responsibility to secure this data lies with the State. A supervisory body or authority should be established to oversee the management of electronic records and devices in police custody. Clarification is also necessary on whether the exemptions granted to the Central Government and its agencies under the Digital Personal Data Protection Act, 2023, extend to law enforcement, and how breaches of personal digital data in police possession will be regulated and addressed. Data collection, such as through the e-FIR system, must be standardized and conducted through secure, government-regulated portals to ensure data integrity. The absence of provisions ensuring the security of electronic evidence raises significant privacy and security concerns, especially given the sensitive data collected under the Criminal Procedure (Identification) Act, 2022. A robust digital infrastructure is needed to prevent potential data breaches.
- **Expansion of Police Authority** The new criminal codes significantly broaden the discretionary powers of the police, particularly concerning the registration of FIRs for non-cognizable offenses following a preliminary inquiry, property attachment, and warrantless arrests. While law enforcement agencies have long sought more authority in these areas, clear guidelines must be established to prevent potential misuse of this expanded discretion. A detailed and stringent code of conduct should be developed to ensure law enforcement remains accountable and exercises these enhanced powers responsibly.

DEVELOPMENTS IN THE FIELD OF DIGITAL FORENSICS IN INDIA

The growing reliance on technology and the rise of digital threats have elevated the significance of digital forensic evidence in modern investigations. Recent legislation emphasizes the role of audio-visual tools in aiding police with crime scene inquiries. These

"audio-visual electronic means" documenting identification procedures, encompass video conferencing, transmitting digital communications, conducting searches and seizures, and other functions as designated by state authorities.
One notable requirement under the new law is the mandatory use of "audio-video electronic means" to record searches and seizures. **Section 105 of the BNSS** mandates that "police officers must record any search or seizure they conduct using audio-video methods. This recording, along with the seizure list, must be submitted promptly to the relevant magistrate, whether district, sub-divisional, or judicial."

Key provisions of the BNSS include:

- For crimes punishable by seven years or more in jail or more, forensic evidence gathering at crime sites is mandated by Section 176(3).
- Ideally, a female officer would collect the testimony of a rape victim in their home or another place of their choosing, with the presence of a parent, guardian, or social worker, as stated in Section 176(1). Audiovisual technology, especially mobile devices, may also capture such evidence.
- Section 180(3) gives the police discretion to record witness statements using audio-video means.
- Section 54 allows for the use of audio-video technology in recording the statements of participants in identification parades when the participant has a physical or mental disability.
- Section 254 permits the use of audio-video technology in session cases to record testimony from witnesses, law enforcement officers, public servants, or experts. Similarly, under Sections 265 and 266, warrant case trials may allow for remote witness examination through state-approved audio-video platforms.
- Section 308 enables the accused to be questioned via audio-video conferencing at locations specified by the state.
- Section 349 expands the scope of forensic evidence collection, as authorized by a magistrate under Section 311A. This includes fingerprints, voice samples, signatures, and handwriting, even from individuals not directly linked to the case under investigation.

With the BNSS now in place, digital forensics in India has taken a giant step forward. In light of the increasing importance of audiovisual evidence in judicial processes, the law specifies procedures for its collection, preservation, and presentation.

Some key advantages of these developments include:

- **Strengthened cybercrime investigations:** Cybercrime investigations and prosecutions may be strengthened with the use of digital forensic evidence.

- **Improved efficiency:** Digital forensic tools enable law enforcement agencies to streamline investigations, saving both time and resources.
- **Increased admissibility:** The likelihood of digital evidence being admissible in court is enhanced by the regulations that have been established for the maintenance of the chain of custody.

However, along with these advancements, the BNSS also introduces challenges:

- **Awareness and training:** Everyone from the general public to solicitors and police officials has to know how to utilise digital forensics correctly in investigations and what the BNSS says.
- **Resource limitations:** Implementing the BNSS requires the establishment of well-equipped digital forensic laboratories, as well as the hiring of skilled personnel and the acquisition of specialized tools.
- **Privacy concerns:** The possibility of privacy breaches and other data breaches increases as investigation procedures become more stringent. Protecting the privacy of both individuals and the nation's data must be prioritised while conducting thorough investigations.

These reforms reflect the increasing role of technology in modern law enforcement and the evolving demands of digital forensics in ensuring justice.

CYBER CRIME PROVISIONS IN INDIA'S NEW LEGAL FRAMEWORK

India's reformed legal system, via the BNS, has implemented extensive steps to combat the increasing prevalence of cybercrimes, underscoring the need to update legislation in response to technological progress. These provisions enhance the current Information Technology (IT) Act by offering comprehensive instructions and imposing more severe penalties to guarantee a vigorous legal response to digital offences.

Section 294 of the BNS addresses the matter of obscene content sent electronically. This clause enforces severe penalties, including incarceration and fines, for those convicted of distributing obscene information online, with even more stringent consequences for repeat offenders. This action seeks to restrict the dissemination of such content online, protecting public decency and morality.

Section 77 pertains to voyeurism, a significant violation of privacy. It imposes penalties for those who photograph or disseminate photos of a woman's intimate parts without her permission. This provision mandates severe repercussions for violations, so safeguard people's privacy and dignity in the digital era. The BNS emphasises the significance of consent and personal privacy by criminalising such actions.

The BNS prioritises cyber theft significantly. **Section 303** explicitly addresses the larceny of mobile devices, data, or computer hardware and software. It ensures victims will get justice by creating a clear legal framework for prosecuting cyber thieves. This section strengthens the IT

Act by fixing loopholes related to digital property theft, making it easier to prosecute and punish such crimes.

Section 78 is crucial in tackling the contemporary offence of cyberstalking. This provision establishes sanctions for both physical and cyber stalking, acknowledging the psychological and emotional damage inflicted by these actions. The BNS seeks to provide a safer online environment by criminalising cyberstalking, especially for at-risk populations like women and children.

The BNS also addresses the possession of stolen digital property. Section 317 imposes penalties on persons possessing stolen mobile phones, computers, or data, regardless of whether they are third parties. This measure diminishes the market for stolen digital products, complicating the ability of hackers to benefit from their unlawful operations.

Some forms of cyber fraud are included under Section 318. These include creating fake websites, stealing passwords, and other similar crimes. The severity of the offence determines the punishment, ensuring that it is proportional to the crime. In light of the alarming increase in cases of internet fraud, this provision provides a strong legal barrier to the practice.

Section 336 addresses email spoofing and online forgeries. Those who engage in email spoofing or forgeries with the intent to harm another person's reputation are subject to the penalties outlined in this section. Through the criminalisation of certain conduct, the BNS seeks to protect individuals from reputational damage and ensure the security of online communications.

STRINGENT MEASURES AGAINST CYBERCRIMES IN INDIA'S NEW CRIMINAL JUSTICE SYSTEM

Inclusion of cybercrime as 'Organised Crime'

'Organised Crime' is defined as a new crime under the New Criminal Laws. It includes cybercrimes and economic offences committed by people or groups operating in concert, either as members or representatives of an organised crime syndicate. A clause that is absent from the IPC is the intention of BNS to prohibit cybercriminals from acting in groups or on behalf of syndicates. While the IPC did mention cybercrimes including data theft and criminal conspiracy, it failed to specifically mention how structured these operations are. In addition, the punishments for cybercrimes have become harsher due to their classification as organised crimes.

Usage of audio-video communications and electronic communication under various procedures

In an effort to reduce the amount of time that criminal trials take, BNSS has incorporated digital technology and allowed the use of "audio-video communications" and "electronic communication" in various court procedures. The goal of this change is to make case information more accessible to everyone involved, reduce paperwork, and make it less inaccurate. The BNSS allows for the electronic service of summonses to witnesses and defendants, the use of audiovisual technology to document statements by investigating officers, the capture of search and seizure operations, and the electronic conduct of trials, enquiries,

appeals, and related proceedings. All crimes, including cybercrimes, may be better enforced and investigated more quickly with this deployment of electronic communications.

Scope of certain sections extended to include activities performed through electronic platforms as crimes

Some provisions of BNS have been expanded to include crimes committed electronically via message or social media platforms, such as extortion, forgery, and hate speech. Therefore, a person's conviction for such crimes may rest on the content of their own messages, emails, and social media posts.

For example, the use of the internet to spread false information that might disrupt public order is now explicitly prohibited under laws against hate speech (Sections 196 and 197 of BNS) and the dissemination of misleading information (Section 353 of BNS). Authorities may now penalise those who incite violence or spread hate using social media or other online platforms. This strengthens enforcement efforts against the growing problems of disinformation and propaganda online, which might lead to civil upheaval. Also, electronically distributed items, such revenge porn or violent films, are now expressly included in definitions, including the interpretation of obscene content under Section 294 of BNS.

In order to improve the legal framework and make it easier to quickly identify cybercriminals who utilise technology and ensure they do not escape punishment, BNS directly incorporates electronic communication in some crucial aspects. Also, for technological ideas that are suggested but not stated clearly in BNS, the Information Technology Act, 2000, and BNSS have been used. Cybercrime detection and prevention will be enhanced by the broader acknowledgement of unlawful behaviour across various digital platforms.

Recognition of electronic records as primary evidence

An enormous step forward in dealing with cybercrimes in India has been made by Section 57 of the BSA. This provision recognises the importance of digital documents, emails, social media posts, and other electronic data as evidence in legal proceedings. In contrast to earlier eras, when such evidence was considered secondary and required further confirmation, this represents a substantial improvement. The investigation and prosecution procedures have traditionally been significantly slowed down by the need for physical copies of digital evidence. Section 57 eliminates this problem by designating electronic documents as major evidence. This makes it easier for courts to review electronic records, which could lead to faster and more efficient case resolutions. This is particularly true in cases involving cybercrime, where multimedia evidence such as digital photographs and videos is often crucial.

The BSA recognises electronic records as main evidence in Section 57, and in Section 63, the protections and particular criteria for the admissibility of such evidence are laid down. Therefore, before being admitted to court, electronic data must meet strict authenticity standards. The following requirements must be met for electronic evidence to be admissible in court, as stated in section 63 of the BSA:

- The computer system that created the record must have functioned properly during the relevant timeframe;
- Data similar to the record must have been consistently input into the system;

- the record must accurately reflect the data entered into it; and
- The computer system must have been used for a lawful purpose during that time.

Furthermore, the provision recognises that the admission criterion may be met by treating data processed by several interconnected devices as a single entity. Finally, a certificate is required for the submission of electronic records as evidence. An expert and the person in charge of the relevant activities' computer or communication infrastructure, or both, must sign this certificate. The admissibility of the records depends on this certificate specifying the procedure, instruments, and equipment used to make them.

The purpose of this is to ensure that electronic evidence is genuine and to stop tainted data from influencing the judicial process. Several instances involving cybercrime rely heavily on digital photographs, videos, and other forms of multimedia evidence. By outlining certain criteria for evidence gathering, preservation, and presentation in court, these suggestions guarantee the reliability of digital multimedia evidence in cybercrime prosecutions. By improving the efficiency of evidence collection, protecting witnesses, and maintaining the integrity of electronic records, this section improves the legal system's ability to tackle cybercrime.

Data privacy concerns

There are concerns about the privacy of individuals involved with the criminal justice system due to the New Criminal Laws' emphasis on electronic evidence and e-governance. While technology has the potential to increase openness and efficiency, it also poses a risk to individuals' right to privacy when their personal information is stored. The security of these electronic records must be guaranteed against intrusion by hackers. To preserve public trust and respect personal privacy rights, the government must build a strong cyber defence system while also enforcing strict privacy safeguards. One provision of the DPDP Act, 2023 that aims to safeguard personal data is the exemption of notice and consent requirements in situations when an offence is being prevented, detected, investigated, or prosecuted. A person has the right to withdraw consent to the processing of personal data under the DPDP Act, but when data is gathered for purposes like criminal investigation, the State is immune to this right.

JUDICIAL TREND

Indian courts have spent a lot of time considering whether or not electronic evidence may be used in court, especially in light of Section 65B of the Indian Evidence Act, 1872. This provision outlines the conditions under which electronic records may be accepted as evidence in court. Indian courts, through a series of landmark judgments, have developed a nuanced understanding of the challenges and protocols surrounding digital evidence. Key decisions have shaped the current framework, emphasizing the critical importance of adhering to legal standards, especially in relation to the certification requirement under Section 65B. This essay examines major judicial rulings that have shaped the use and admissibility of digital evidence, highlighting the judiciary's evolving approach towards balancing the need for technological advancements and the safeguarding of due process.

The landmark case of "State (NCT of Delhi) v. Navjot Sandhu", also known as the Parliament Attack case, was one of the earliest instances where the Supreme Court of India dealt with the issue of the admissibility of electronic records. In this case, the Court was faced with the question of whether call records could be admitted as evidence without the certificate required under Section 65B (4). The Court held that "electronic records could be admitted as evidence even in the absence of a certificate under Section 65B, provided the original electronic document was produced." The judgment seemed to create a lenient framework for the admissibility of digital evidence, allowing the courts to accept electronic records without insisting on the mandatory certification.

However, this decision was later criticized for diluting the rigorous safeguards prescribed by the Indian Evidence Act to ensure the authenticity of electronic records. The Court's ruling in Navjot Sandhu led to ambiguity regarding the proper procedure for admitting digital evidence, and this issue persisted until it was revisited in subsequent cases.

A significant shift in the judiciary's approach to electronic evidence came in the case of "Anvar PV v. PK Basheer", which overruled the Navjot Sandhu judgment. The Supreme Court in India ruled categorically that electronic documents cannot be admitted without a certificate issued under Section 65B(4) of the Indian Evidence Act. The Court has made it clear that this certificate is necessary in order to accept electronic evidence. It must attest that the electronic record was created by a trustworthy computer system, as specified in Section 65B (2). In order to maintain the credibility and validity of electronic evidence, this ruling reiterated the need to follow rigorous procedural rules. The importance of the certificate as a protection against digital evidence modification and fabrication was highlighted by the Court in the Anvar PV case. Digital records were strengthened in their evidential value by the Court's decision to reinstate the certificate's required character. This meant that digital records could only be accepted with a suitable certification attesting to their authenticity and conformity with Section 65B's technical standards.

In "Manu Sharma v. State (NCT of Delhi)", commonly referred to as the Jessica Lal murder case, digital evidence played a pivotal role in securing the conviction of the accused. The case involved the use of digital footage and mobile phone records to establish the presence of the accused at the crime scene and to reconstruct the sequence of events leading up to the murder. This case highlighted the increasing reliance on digital evidence in modern criminal investigations and its critical role in establishing guilt.

Although the case predates Anvar PV, it showcased the potential of digital evidence to play a decisive role in high-profile criminal cases. The use of digital evidence in Manu Sharma demonstrated its capability to bolster the prosecution's case and ensure that justice is served, marking an important step in the Indian judiciary's recognition of the evidentiary value of electronic records.

In "Unnikrishnan v. State," the Madras High Court ruled that digital photographs constitute primary evidence and do not require the submission of negatives for authentication, provided they comply with Section 65B of the Evidence Act. This decision marked a significant development in the use of digital evidence, particularly in cases where physical negatives of

photographs were no longer available due to advancements in digital photography. The Court recognized the importance of adapting legal standards to accommodate technological progress, while still ensuring that the procedural requirements under Section 65B were followed to safeguard the authenticity of digital photographs.

The case of "K Ramajayam v. Inspector of Police" reaffirmed the principles laid down in Anvar PV, particularly the mandatory requirement of a certificate for electronic records. The Court ruled against the admissibility of electronic evidence in the absence of certification, underscoring that external evidence could not be used to fill the gap. This decision further cemented the legal precedent set by Anvar PV, ensuring that the admission of electronic records in court strictly adhered to the provisions of Section 65B.

In "P Gopalkrishnan v. State of Kerala", The Supreme Court addressed the issue of an accused's right to access electronic records. The case involved electronic records stored on memory cards and pen drives. The Court held that such records are to be treated as "documents" under the Indian Evidence Act, and the accused must be given access to cloned copies of these records to prepare their defence. However, the Court also recognized the need to balance this right with privacy concerns, ruling that access should be granted in a restricted manner under court supervision.

This decision reinforced the Court's commitment to ensuring fairness in criminal trials, emphasizing the need for transparency in the use of digital evidence while also safeguarding the privacy of individuals. It provided clarity on the accused's rights in relation to digital evidence, ensuring that they have a fair opportunity to challenge the evidence presented against them.

The "Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal" The case reiterated the mandatory nature of the Section 65B certificate for the admissibility of electronic records. The Supreme Court ruled that unless a certificate is produced at the time of submitting electronic evidence, such records cannot be admitted. This judgment reinforced the precedent set in Anvar PV and emphasized the need for strict compliance with the procedural requirements outlined in the Evidence Act.

THE WAY FORWARD

The BNSS represents a notable step in the incorporation of digital forensics into India's judicial system. The new legislation makes it easier to investigate cybercrime by highlighting the value of audiovisual evidence and setting clear guidelines for its collection, storage, and presentation in court proceedings. But there are a number of areas that need more improvement before India can fully benefit from digital forensics.

The public, attorneys, and law enforcement all need a better understanding of digital forensics and its role in the judicial system. For digital forensics to continue to evolve, researchers must work to increase collaboration between academia, businesses, and law enforcement. The worldwide nature of cybercrime makes strong international cooperation in the pursuit of evidence and the punishment of offenders very necessary. By addressing these issues, India

can ensure that digital forensics makes a substantial contribution to the administration of justice and the enforcement of laws in the digital age.

Defamation, especially via digital platforms, is addressed under Section 356. This clause penalises the transmission of defamatory information by email, with penalties that include incarceration and monetary fines. By tackling digital defamation, the BNS safeguards people's reputations in the online realm, underscoring the increasing significance of digital communications.

These parts jointly enhance the legal framework's capacity to pursue cybercrimes successfully. They provide comprehensive rules and rigorous sanctions, ensuring that the legal system can tackle the intricacies of contemporary digital crimes. The BNS enhances the current IT Act, providing a thorough legal framework to address cybercrimes and protect persons and organisations from the escalating hazards of digital technology. This comprehensive strategy demonstrates the Indian government's dedication to modernising its legislative framework and ensuring strong safeguards in a progressively digital environment.

CONCLUSION

India's new criminal law reforms, namely the Bhartiya Nyay Sanhita (BNS), Bhartiya Nagarik Suraksha Sanhita (BNSS), and Bhartiya Sakshya Adhiniyam (BSA), mark a significant leap forward in addressing the growing challenges of cybercrime and the relevance of digital forensics in legal processes. These reforms reflect the nation's acknowledgment of the increasing role of technology in both criminal activity and investigations, responding to the complexity of modern cybercrimes with updated provisions and tools that align with global standards.

A significant achievement resulting from these changes is the thorough incorporation of digital forensics into the criminal justice system. The BNSS increases openness and accountability by authorising the use of video technology in police investigations, including the recording of searches, seizures, and witness testimony. The mandate for collecting forensic evidence at crime scenes for serious offences enhances the integrity of investigations, guaranteeing that digital evidence is both admissible and essential in legal processes.

The transition to acknowledging digital records and electronic evidence as main evidence under the BSA is a significant advancement that recognises the essential importance of digital data in modern judicial proceedings. The comprehensive standards for the acceptance of digital evidence provide explicit instructions for verifying its validity and maintaining the chain of custody, therefore enhancing the likelihood of obtaining convictions in cybercrime cases.

Nevertheless, the execution of these measures presents obstacles. Comprehensive training for the public, legal professionals, and law enforcement in digital forensics is essential for the effective implementation of these laws. Moreover, the creation of well-equipped digital forensic labs, together with the hiring of proficient professionals, would be crucial in addressing the technological requirements of contemporary investigations.

A significant issue is the equilibrium between expanded investigative authority and the safeguarding of personal privacy. The extensive powers conferred upon law enforcement,

especially regarding the confiscation of electronic devices and data, engender significant privacy concerns that need vigilant control to avoid misuse. As investigations increasingly depend on digital evidence, protecting personal data and guaranteeing adherence to privacy regulations will be essential for preserving public confidence.

BNS, BNSS, and BSA together signify a substantial modernisation of India's legal system, enhancing its responsiveness to the issues posed by the digital era. Although these changes provide essential legislative instruments to tackle cybercrime successfully, their efficacy will hinge on ongoing initiatives to educate stakeholders, enhance technological infrastructure, and preserve a judicious equilibrium between law enforcement authority and individual rights. With these steps implemented, India is poised to enhance its cybercrime prevention strategies and guarantee the administration of justice in a more digital landscape.

References

1. Kshetri, Nir. Cybercrime and Cybersecurity in India. Routledge, 2021.
2. Bansal, Vivek Sood. Cyber Laws in India: IT Act 2000 & Beyond. LexisNexis, 2016.
3. Harisha, A., et al. "Advancements in Cybercrime Investigation and Digital Forensics" (CRC Press, 2023).
4. Meshram, et al. "Medical Forensics Principles and Cyber Crime Forensic Investigation Model." (2024)
5. Pavan Duggal. Digital India: Reflections on IT Laws. Universal Law Publishing, 2019.
6. Jaitley, A., & Bhushan, C. Cyber Laws in India: An Analysis. Eastern Book Company, 2022.
7. Ashok Kumar. Digital Forensics in Indian Context. Regal Publications, 2023.
8. Sinha, Manish Kumar. "Digital Forensics: Challenges and Legal Perspectives in India." Journal of Indian Law and Society, vol. 12, no. 2, 2022, pp. 145–163.
9. Bhattacharjee, Arundhati. "Emerging Legal Framework for Cybercrime in India: New Criminal Laws and Forensics." Indian Journal of Law and Technology, vol. 19, 2024.
10. Chopra, Rishi. "Admissibility of Electronic Evidence: Evolution under India's New Bharatiya Sakshya Adhiniyam." NUJS Law Review, vol. 16, no. 1, 2025.
11. Mishra, P., & Kumar, S. "Legal Aspects of Cyber Forensics: An Indian Perspective." International Journal of Cyber Criminology, vol. 13, 2021.
12. Ministry of Home Affairs, Government of India. Handbook on Cybercrime Investigation. MHA Cyber & Information Security Division, 2023.
13. Ministry of Law and Justice. Explanatory Note on the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita & Bharatiya Sakshya Adhiniyam. 2024.
14. National Crime Records Bureau (NCRB). Crime in India Report 2023: Cybercrime Statistics. NCRB, 2024.
15. CERT-In (Indian Computer Emergency Response Team). Annual Report on Cyber Incidents and Response in India. MeitY, 2024.
16. Bharatiya Nyaya Sanhita, 2023 (BNS) — replacing IPC; contains provisions on cyber fraud, identity theft, data breaches.
17. Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) — procedural law, including provisions for search, seizure, and preservation of electronic evidence.
18. Bharatiya Sakshya Adhiniyam, 2023 (BSA) — replacing Indian Evidence Act; significantly updates rules on electronic records, chain of custody, and admissibility.

19. Information Technology Act, 2000 (as amended) — primary legislation governing cyber offenses, digital signatures, and electronic evidence.
20. Sood, Vivek. Cyber Laws in India: IT Act 2000 & Beyond. LexisNexis, 2016.
21. Bhattacharjee, Arundhati. "Emerging Legal Framework for Cybercrime in India: New Criminal Laws and Forensics." Indian Journal of Law and Technology 19 (2024): 1–22.
22. Ministry of Law and Justice. Explanatory Note on the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita & Bharatiya Sakshya Adhiniyam. Government of India, 2024.
23. Ministry of Home Affairs, Government of India. "Cyber & Information Security Division." Accessed July 2025. https://cis-mha.gov.in.
24. R.K. Suri & T.N. Chhabra. Cyber Crime In India. Pentagon Press, 2018.
25. Debarati Halder & K. Jaishankar. Cyber Crime and The Victimization of Women: Laws, Rights and Regulations. IGI Global, 2016.
26. Alok Kumar. Practical Guide to Cyber Laws with Cyber Security and Forensics. Taxmann, 2020.
27. Anirban Sengupta. Digital Evidence: A Practitioner's Handbook. Oakbridge, 2021.
28. Bhattacharya, Paroma. "Digital Evidence and Indian Courts: Admissibility, Authenticity, and Integrity In The Age of BSA." Indian Law Review, Vol. 9, No. 1, 2025.
29. Rai, Neha. "Digital Forensics in India: Bridging The Legal and Technological Gap." Cyber Law Journal of India, Vol. 7, 2023.
30. Prasad, R. "India's New Criminal Laws and Cybercrime: Scope And Challenges." Journal of Cyber Policy, Vol. 8, 2024.
31. Gupta, A., & Sharma, R. "Procedural Challenges in Collecting Electronic Evidence In India." Law & Technology Review, Vol. 6, 2024.
32. Niti Aayog. National Strategy for Artificial Intelligence & Cyber Security. Government Of India, 2023.
33. Data Security Council Of India (DSCI). Study On Challenges in Cybercrime Investigation in India. DSCI Whitepaper, 2023.
34. Law Commission of India. Report No. 279: Review of Evidence Act with Reference to Electronic Evidence. Law Commission, 2022.
35. CBI Cyber Crime Investigation Manual. Central Bureau of Investigation Handbook for Digital Forensics & Cybercrime. CBI, 2021.
36. Supreme Court of India. State Of Delhi Vs. Mohd. Afzal & Others (2003) – Digital Evidence and Authenticity Issues.
37. Supreme Court of India. Arjun Panditrao Khotkar Vs. Kailash Kushanrao Gorantyal (2020) – Clarifying Section 65b Certificate Requirements Under The Evidence Act.
38. Sengar, Sanket Singh. "From Pixels to Policies: Analysing the Provisions and Navigating the Complexities of the Digital Personal Data Protection Act, 2023." (2023) SSRN 4547842.