NFSU JOURNAL OF FORENSIC JUSTICE

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

BYTES AND RIGHTS: UNPACKING SEARCH AND SEIZURE OF THE ELECTRONIC EVIDENCE UNDER INDIA'S LEGAL FRAMEWORK

Devansh Malhotra[1], Rohit Kumar Shrivastava[2]

Abstract: *The increasing prevalence of cybercrimes has clamoured a robust legal framework for the search, seizure, and admissibility of electronic evidence in India. The Information Technology (IT) Act, 2000, along with provisions under the Bharatiya Nagarik Suraksha Sanhita, 2023 (previously Code of Criminal Procedure, 1973), and the Bharatiya Sakshya Adhiniyam, 2023 (previously Indian Evidence Act, 1872), governs the legal parameters of digital evidence collection, preservation and unimpeachable chain of custody in investigation. However, various problems persist in leveraging law enforcement's investigative powers coupled with the constitutional safeguards, particularly the Right to Privacy and the Right to a Fair Trial granted under Article 21 of the Constitution of India. This paper examines the legal framework governing search and seizure under the IT Act, 2000 and general provisions of the Bharatiya Nagarik Suraksha Sanhita, 2023 as applicable, analysing the scope, limitations, and judicial precedents of these provisions in a complex legal framework. It also explores the interplay between legal mandates and forensic methodologies, emphasising compliance with sections 61 and 63 of the Bharatiya Sakshya Adhiniyam, 2023, which delineates admissibility requirements for electronic records. This paper further addresses due process concerns, including the requirement of special judicial warrants, challenges in cross-border digital investigations, and procedural gaps in handling encrypted and cloud-based data including digital personal data. Furthermore, the paper discusses challenges such as encryption barriers, electronic evidence retrieval, and the exigency for a comprehensive National Cyber Forensic Policy, comparing India's approach with global best practices from the US, UK, and EU Cybersecurity laws. The paper also refers to key judicial precedents, both Indian and International, that have shaped the legal contours of digital search and seizure. In addition to it, a comparative analysis with the US Electronic Communications Privacy Act, 1986 (ECPA) and the UK's Investigatory Powers Act, 2016 highlights best practices for balancing state surveillance powers with individual rights. Considering the fact of decolonising Indian criminal laws, both substantive and procedural, and leaving this crucial aspect unaddressed creates a policy vacuum. Finally, the paper proposes legislative and procedural reforms, for strengthening forensic integration in search and seizure operations, including capacity-building for all stakeholders namely judicial sensitisation including that of Public Prosecutors, personnel of Law Enforcement Agencies; a National Framework for Cyber Forensic and Digital Evidence handling, and stricter compliance mechanisms for Law Enforcement Agencies, ensuring that search and seizure in the cases involving digital evidence and cyberspace, aligns with constitutional principles and international legal standards.*

Keywords: *Electronic Evidence, Search and Seizure, IT Act 2000, Bharatiya Sakshya Adhiniyam 2023, Cyber Forensics.*

INTRODUCTION

In today's digital age, electronic evidence has emerged as a cornerstone in both civil and criminal matters, making its proper handling *sine qua non* for effective justice delivery and its administration. However, the procedures for the search and seizure of electronic evidence in India continue to face significant challenges. Existing methods are governed by the Bhartiya Sakshya Adhiniyam, 2023[1] ["BSA"] (replaced Indian Evidence Act, 1872[2]), Bhartiya Nagarik Suraksha Sanhita, 2023[3] ["BNSS"] (replaced Code of Criminal Procedure, 1973[4]) and the

[1] LLM Student, NLIU Bhopal.
[2] Final year MCLIS Student, NLIU Bhopal.
[1] Bharatiya Sakshya Adhiniyam 2023 (48 of 2023).
[2] Indian Evidence Act 1872 (01 of 1872).
[3] Bharatiya Nagarik Suraksha Sanhita 2023 (46 of 2023).
[4] Code of Criminal Procedure 1973 (02 of 1974).

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

Information Technology Act, 2000[5] (IT Act). Although these provisions offer some direction, since provisions are draped and dealing with general issues, a lack of a complete framework has caused differences in interpretation terms and the procedural loopholes in dealing with the contemporary issues related to the paradigm of search and seizure of cyber evidence.

The constantly changing technological terrain adds another level of challenges, as law enforcement bodies find it hard to keep up with advancements in the data storage, encryption, and communication technology. This tends to lead to mishandling of electronic evidence, thus tainting it and making it inadmissible in the courts. Additionally, the search and seizure process tend to include the retrieval of personal information of the accused or suspect, raising serious privacy issues while striking a balance between the interest of the state in crime prevention and control. Striking a balance between the rights of the accused and the need to obtain evidence for judicial examination is an urgent concern which highlights the necessity for procedures that are standardised and are clear and unambiguous in terms of interpretation. In addition, such procedures must also be harmonious with the other rights of the accused/suspects extended either under the constitution or provisions of statutes that are regular. One of the most important considerations in overcoming such challenges is documenting and maintaining proper electronic evidence for ensuring its sanctity. Without any of the standardised procedures in these issues, there can be doubt raised about the chain of custody of such evidence that may undermine such evidence's admissibility as evidence in the court of trial. Hence, establishing strong frameworks in regulating search and seizure while preserving the privacy and data protection principles is quintessential for filling such gaps.

In this environment, cyber forensics has a key role to play in guaranteeing the integrity, authenticity, and reliability of electronic evidence. Cyber forensic professionals employ various sophisticated tools and methods to identify, capture, preserve, analyse, and present electronic information while adhering to technical and legal standards. Their skill is vital in retrieving erased files, decrypting encrypted information, and retrieving information from the broken devices—all of which are central in the investigation process.

Cyber forensic techniques focus on producing forensic images and obtaining hash values of the seized devices to guarantee data integrity and avoid tampering. Moreover, the use of forensic tools guarantees the systematic recovery of evidence and keeps it in its original form, thereby preserving its validity for judicial examination. Also, suitably trained forensic experts contribute significantly towards reducing procedural errors and enhancing the evidentiary strength of digital artifacts recovered from the accused/suspects.

In order to counter these challenges efficiently, India must have a multi-pronged strategy, encompassing the development of standardised legal systems integrating cyber forensic methods, investment in the cutting-edge forensic technology, and conducting training programmes to train and equip the law enforcement officials with appropriate skills to tackle search and seizure of electronic evidence. In addition, while embedding privacy protections and ethical considerations in these frameworks will balance investigative requirements with individual rights protection, thereby building faith in the legal system's capability to manage the electronic evidence efficiently. Through the use of and the harnessing of cyber or digital forensics combined with revised legal and procedural directives, India can improve its ability to respond to the challenges of digital evidence under contemporary investigations.

STATUTORY AND LEGAL FRAMEWORK GOVERNING ELECTRONIC EVIDENCE

India's legislative framework of laws governing the investigation and admissibility of electronic evidence has undergone tremendous change with the enactment of the BNSS, the BSA, and the continued application of the IT Act. When they are read together, these enactments provide a firm basis for a framework to address the growing dominance and use of digital evidence particularly in criminal proceedings before the courts.

Under the BNSS, there have been various provisions made or reworked for the purpose of procedural justice and technological flexibility. Such as section 94[6] authorises investigating authorities to serve summons or orders for the production of documents and electronic messages, so as to legitimise digital forms as

[5] Information Technology Act 2000 (21 of 2000).

[6] Bharatiya Nagarik Suraksha Sanhita 2023 (46 of 2023), s. 94.

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

original sources of evidence. Section 105[7] requires the audio-visual recording of search and seizure operations, so as to ensure transparency and avoid the misuse of authority in the context of such operations. Section 106[8] enables the seizure of property suspected to be linked to the commission of a crime, including electronic devices. Further, section 176 (3)[9] introduces a hierarchical mechanism for reporting progress in investigations, promoting accountability, alongside promoting the use and integration of forensics in crime scene investigation. In a major shift towards digitisation, section 530[10] expressly allows the conduct of trials and proceedings in electronic mode, reflecting the legislature's intent to modernise India's criminal justice process.

The BSA supports this procedural code by legislating evidentiary principles with regard to electronic records. Section 58[11] describes secondary evidence, which is highly applicable when there are copies or outputs from electronic sources. Section 61[12] positively recognises that electronic and digital records are admissible as evidence and puts them at par with common documentary evidence. In order to preserve authenticity, section 63(4)[13] requires a certificate on prescribed conditions—similar to the previous section 65B[14] of the Indian Evidence Act, 1872—when submitting computer-generated records, thus preventing tampering and maintaining evidentiary reliability.

In the meantime, the IT Act, 2000 performs a vital regulatory function. Section 69A[15] authorises the Central Government to block access to digital content in the interest of sovereignty, integrity, national security, and public order. Section 80[16] also authorises specified police officers to enter, search, arrest, and seize electronic evidence without warrant in certain cases under the Act, thus dealing with the real-time nature of cyber offences.

The CBI Manual on Digital Search and Seizure[17] provides a systematic framework for ensuring that digital evidence is obtained legally, in a transparent manner, and without infringing upon the rights of citizens. Its procedural safeguards are especially pertinent in light of the increasing concern over the intrusive character of computer searches. The Manual makes officers seek proper authorisation prior to conducting any search and keep in-depth reasons for doing so, which reinforces accountability in them. The searches have to be conducted in the presence of the independent witnesses, which helps preserve the integrity of the process and provide an impartial safeguard against abuse or falsification. One of the most critical aspects of the Manual is its emphasis on data integrity—officers need to calculate and keep the hash values of the digital devices at the time of seizure of the evidence, so that the digital content is not touched and can also withstand the test of judicial scrutiny. In addition, it mandates that an itemised seizure memo be done on site of the search, detailing all the items seized and their details, with a copy given to the individual concerned, thereby improving documentation and transparency.

The CBI Manual harmonises with the procedural protections embedded in the Code of Criminal Procedure so that the digital search and seizure process is in conformity with constitutional guarantees like the right to privacy and the right against self-incrimination. In December 2023, the Supreme Court, while observing that there was no uniform statutory requirement for seizing electronic devices, ordered all the central investigating agencies to follow the guidelines set down in the CBI Manual till such time that an overarching legal regime is codified. Judicial acknowledgement of the Manual as a provisional standard validates its significance and positions it as an important document in protecting digital rights.[18] It is even more important when harmonised with other regulatory writings such as the Central

[7] Bharatiya Nagarik Suraksha Sanhita 2023 (46 of 2023), s. 105.
[8] Bharatiya Nagarik Suraksha Sanhita 2023 (46 of 2023), s. 106.
[9] Bharatiya Nagarik Suraksha Sanhita 2023 (46 of 2023), s. 176 (3).
[10] Bharatiya Nagarik Suraksha Sanhita 2023 (46 of 2023), s. 530.
[11] Bharatiya Sakshya Adhiniyam 2023 (48 of 2023), s. 58.
[12] Bharatiya Sakshya Adhiniyam 2023 (48 of 2023), s. 61.
[13] Bharatiya Sakshya Adhiniyam 2023 (48 of 2023), s. 63 (4).
[14] Indian Evidence Act 1872 (01 of 1872), s. 65B.
[15] Information Technology Act 2000 (21 of 2000), s. 69A.
[16] Information Technology Act 2000 (21 of 2000), s. 80.
[17] CBI Manual on Handling of Electronic Evidence (Central Bureau of Investigation, Government of India 2020) <https://cbi.gov.in> accessed 05 April 2025.
[18] *Foundation for Media Professionals v Union of India and Ors.*, W.P. (Cri.) No. 395 of 2022.

NFSU JOURNAL OF FORENSIC JUSTICE

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

Board of Direct Taxes (CBDT) Manual[19] or IT Act, 2000, guidelines so creating part of an overall digital due process system. Given increased digital surveillance and resultant heightened evidentiary dependency upon electronic evidence, the CBI Manual, 2020[20] is the bulwark against arbitrariness, yet ensuring evidentiary integrity of investigations and adherence to the constitution.

The proposed Income Tax Code, 2025[21] introduces expansive powers for tax authorities in relation to digital search and seizure, raising significant legal and constitutional concerns. While the Code attempts to modernise enforcement in the digital era, it risks deviating from the procedural safeguards currently enshrined in the CBDT Investigation Manual.[22] The Manual, though administrative in nature, issued under section 119 of the Act[23], lays down essential procedural checks—such as maintaining data integrity, creating mirror images of seized devices in the presence of independent witnesses, and securing devices with hash value verification. These safeguards are designed to prevent misuse, ensure evidentiary reliability, and protect individual rights during search operations involving electronic evidence.[24]

However, the proposed Direct (Income) Taxes Code, 2025[25], in its current form, does not incorporate these well-established procedural protections as binding legal requirements.[26] The lack of statutory recognition for protocols on device imaging, digital evidence chain-of-custody, or oversight during forensic extraction poses risks of arbitrary enforcement. Civil liberties groups, including the Internet Freedom Foundation (IFF), have raised concerns that such unchecked powers may infringe on the constitutional right to privacy under Article 21[27], especially in the absence of judicial oversight or clearly defined legal thresholds for digital intrusions.[28]

The CBDT Manual recognises the sensitive nature of digital evidence and mandates caution, confidentiality, and proportionality—principles echoed in global standards for digital forensics. The proposed Code, however, does not offer explicit statutory safeguards to uphold these principles. Critics argue that codifying these safeguards within the new law is essential to ensure compliance with due process and constitutional mandates. While there is merit in equipping authorities to tackle sophisticated digital tax evasion, such enforcement must operate within a framework of necessity, proportionality, transparency, and accountability. In sum, for the Income Tax Code, 2025 to be both effective and constitutionally compliant, it must harmonise its enforcement provisions with the procedural rigour already laid down in the CBDT Manual and supported by constitutional jurisprudence.

In the case of *Dharambir v CBI*[29], the Delhi High Court in the light of the broad definitions of 'document' and 'evidence' under the amended section 3 of the Indian Evidence Act,1872 (IEA), when read with sections 2(o) and 2(t) of the Information Technology Act, 2000, a hard disk that has undergone any form of alteration qualifies as an "electronic record". Consequently, it would fall within the meaning of a 'document' as per section 3 of the IEA. Also, now the Bharatiya Sakshya Adhiniyam, 2023 (BSA) by the virtue of section 2 (d) and section 2 (e) makes the definition of 'document' and 'evidence' inclusive so as to include digital and electronic records. Courts in various instances have relied upon the digital forms of evidence like a series of documents exchanged and authenticated by the parties, such as emails, letters, telex, telegrams, and other forms of

[19] Central Board of Direct Taxes, Digital Evidence Investigation Manual (National Academy of Direct Taxes 2014) <https://nadt.gov.in/writereaddata/MenuContentImages/digital-evidence-investigation-manual-20146385320454754220.pdf> accessed 05 April 2025.

[20] *CBI Manual* (n 19).

[21] *The Direct Taxes Code Bill 2025* (Bill No. 24 of 2025, introduced in Lok Sabha, Ministry of Finance, Government of India) <https://incometaxindia.gov.in/Documents/income-tax-bill-2025/income-tax-bill-2025.pdf>accessed 05 April 2025.

[22] *CBDT Manual* (n 21).

[23] The Income Tax Act 1961 (43 of 1961), s. 119.

[24] *M/s. Saravana Selvarathnam Retails Private Limited v Commissioner of Income Tax Appeals*, 2024 LiveLaw (Mad.) 101; W.P. Nos. 9753, 9757, 9761 and 11176 of 2023.

[25] *The Direct Taxes Code Bill 2025* (n 23).

[26] *The Direct Taxes Code Bill 2025* (n 23), cl. 247, 474.

[27] Constitution of India 1950, art 21.

[28] Internet Freedom Foundation, 'IFF writes to the Select Committee to review the digital search and seizure powers under the Income Tax Bill, 2025' (Internet Freedom Foundation, 1 April 2025) <https://internetfreedom.in/iff-writes-to-the-select-committee-to-review-the-digital-search-and-seizure-powers-under-the-income-tax-bill-2025/> accessed 05 April 2025.

[29] 148 (2008) DLT 289.

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

telecommunication, can help infer the existence of contract, even in the absence of a formally signed agreement.[30] Such an approach is an *agenda regularis* in cases of '*dawn raids*' conducted by the antitrust regulator in India and across the globe.[31] The Investigators under the Competition law now are vested with the powers to search and raid the premises and seize *all* the evidence in form of books, papers, devices, etc. relevant to said violation as for which the warrant is issued.[32] Drawing from the *ratio* laid down in *Dharambir* and new provisions of BSA which talk about the definition of document and evidence, most of the records of the establishments are stored in the form of electronic records in databases, hard drives, pen-drives, etc. the said provision(s) enable the antitrust regulators to seize the same as a wholesale measure, and that too without any judicial application of mind.

In the case of *Sanjay Kumar Kedia v Narcotics Control Bureau and Anr.*[33], the intersection of NDPS Act and IT Act, where Xponse Technologies Ltd. and Xpose IT Services Pvt. Ltd., led by Sanjay Kedia, were found to have created, hosted, and operated pharmaceutical websites through which large quantities of psychotropic substances, namely Phentermine and Butalbital, were illegally distributed in the United States. These activities were facilitated with the assistance of various associates. Investigations revealed that the operations were carried out using the IP address 203.86.100.76, which was traced back to the company's digital infrastructure. The case highlighted the misuse of technology and digital platforms for transnational drug trafficking and raised serious concerns about the regulation of online pharmaceutical sales. The incident underscores the need for stringent monitoring of cyber activities and international cooperation to curb the online distribution of controlled substances. The Court while applying the long arm principle in this case repelled the contention of the Petitioner that he was merely an intermediary in the transactions, hence squarely within the scope of section 79 of the IT Act; the Court negatived this contention by ruling that section 79 of the IT Act only extends to offences under that Act and not others *inter alia*. In summary, the changing statutory and legal paradigm regulating electronic evidence in India is a progressive catching up with advancing technology and the demands of justice. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA), and the Information Technology Act, 2000 altogether provide a systemic legal framework for identifying, collecting, and receiving electronic records. These laws include not only vital safeguards such as procedural standards, certification requirements, and public openness in search and seizure, but they also manifest a thoughtful, considered step towards the modernisation of investigation and evidentiary practices. Nevertheless, despite this codification, enforcement and application of these provisions remain largely subject to judicial control. Courts have been in the vanguard of developing privacy, admissibility, and authenticity standards of electronic evidence, often walking the thin line between constitutional rights, the technical nuances, and the procedural justice. Thus, to have a holistic understanding of the efficacy and challenges of such a legal framework, it becomes quintessential to examine judicial interpretations and precedents that have shaped the *de facto* implementation of the electronic evidence norms. The subsequent chapter on Judicial Trends and Analysis seeks to unravel this vital convergence of law and technology through the lens of case law, hence placing statutory provisions in real adjudicatory settings.

JUDICIAL TRENDS AND ANALYSIS ON SEARCH AND SEIZURE OF ELECTRONIC EVIDENCE

The legal scenario involving the admissibility of electronic evidence has dramatically changed, and the courts are struggling to tackle concerns of the digital information, e-surveillance, and privacy. Various judicial precedents in India and the common law countries like the United Kingdom (UK) and the United States of America (USA) have been instrumental in

[30] *Trimex International FZE Ltd. v Vedanta Aluminium Ltd. India*, (2010) 3 SCC 1; *Shakti Bhog Foods Ltd. v Kola Shipping Ltd.*, (2009) 2 SCC 134.
[31] Devansh Malhotra and Vaibhav Garg, 'Whether the Presence of a Lawyer is Essential During a Dawn Raid by the Competition Regulators' (SCC Online, 18 January 2023) <https://www.scconline.com/blog/post/2023/01/18/whether-the-presence-of-a-lawyer-is-essential-during-a-dawn-raid-by-the-competition-regulators/> accessed 31 March 2025.
[32] The Competition Act 2002 (12 of 2003), s. 41 (3) and 41 (4).
[33] (2009) 17 SCC 631.

influencing the rule of regulation relating to the search, seizure, and evidentiary admissibility of the computer data. The development of jurisprudence can be traced by milestone cases exemplifying dynamics of technological advancement and the legal safeguards.

One of the first and most landmark decisions concerning electronic evidence came in *R v Maqsud Ali*[34], where the United Kingdom Court of Appeal addressed the admissibility of secretly tape-recorded conversations in a criminal trial. The Court held that such recordings are admissible if their correctness and authenticity can be proven. Such a ruling cleared the way to the acceptance of electronic evidence as an effective proof with proper attention being paid to procedural safeguards to check tampering and forgery. The present ruling became the vital precedent of Indian law, and subsequent judgements on electronic evidence, especially when audio and video recordings came into play.

Electronic evidence law further developed with *R v Robson*[35], where the issue of warrantless search and seizure was examined. The court held that a warrantless search would be constitutional if the accused person had voluntarily agreed to it, subject to the condition that such consent should not be induced by coercion, and any such evidence discovered in derogation of due process standards would be unacceptable. This case is of particular importance in the Indian context, where the procedure of search and seizure is governed by the Bharatiya Nagarik Suraksha Sanhita, 2023 (which has replaced the Code of Criminal Procedure, 1973). The principles laid down in *R v Robson*'s finding is heard in the Indian legal system, where there has to be observance by police authorities of procedural safeguards while obtaining electronic evidence so that constitutional rights can be sustained.[36]

In the *United States v Richards*[37], the U.S. courts emphasized the necessity of narrowly crafted warrants to avoid arbitrary digital searches, reaffirming the protections of the Fourth Amendment. This was followed in *Riley v California*[38], when the US Supreme Court imposed a warrant requirement for retrieving cell phone data after arrest, in light of the vast personal data that is stored digitally. To this, *United States v Young*[39] reaffirmed the third-party doctrine, deciding that voluntarily disclosed data to service providers is stripped of privacy protection, pointing to a lacuna that India's law needs to fill in the wake of the Digital Personal Data Protection Act, 2023.[40] Likewise, *US v Walser*[41] reiterated that general warrants allowing indiscriminate searches of digital material are constitutionally invalid and require specificity and proportionality. In India, drawing parallels from the Supreme Court decision in *Ritesh Sinha v State of Uttar Pradesh*[42] allowed for the taking of voice samples but required legislative protection to preserve privacy, previewing difficulties with coerced access to digital technology. Concurrently, in the case of *Dharam Deo Yadav v State of Uttar Pradesh*[43], the Supreme Court underscored the use of scientific and procedural diligence when dealing with criminal cases and crime scene management, considering its ever-evolving developments which help the courts to increase the probative value of evidence obtained using such means.

The 'reasonable expectation of privacy' doctrine, established in *Katz v United States*[44], expanded constitutional protections to electronic communications, ruling that warrantless government surveillance violated the Fourth Amendment. This principle significantly influenced *PUCL v Union of India*[45], where the Supreme Court of India recognized privacy as a fundamental right under Article 21, limiting arbitrary state surveillance using telephone tapping. The doctrine is particularly relevant for search and seizure of electronic devices, which contain sensitive personal data, requiring clear legal safeguards. Another crucial precedent in digital search jurisprudence is the 'Doctrine of Foregone Conclusion', propounded in *Fisher v United States*[46], which holds that if law enforcement

[34] *R v Maqsud Ali* [1965] 2 All ER 464 (CA).
[35] *R v Robson* [1972] 2 All ER 699 (CA).
[36] *PUCL v Union of India*, (1997) 1 SCC 301; *KS Puttaswamy v Union of India,* (2017) 10 SCC 1.
[37] *United States v Richards*, 659 F3d 527 (6th Cir 2011).
[38] *Riley v California*, 573 US 373 (2014).
[39] *United States v Young*, 350 F3d 1302 (11th Cir 2003).
[40] Digital Personal Data Protection Act 2023 (22 of 2023).
[41] *United States v Walser*, 275 F3d 981 (10th Cir 2001).
[42] (2019) 8 SCC 1.
[43] (2014) 5 SCC 509.
[44] *Katz v United States*, 389 US 347 (1967).
[45] *PUCL* (n 35).
[46] *Fisher v United States*, 425 US 391 (1976).

already knows the existence and location of evidence, compelling its production does not violate the Fifth Amendment right against self-incrimination.

The experience of the Indian judiciary with electronic evidence changed inexorably with *Ram Singh & Others v Col. Ram Singh*[47], wherein the Supreme Court of India discussed the admissibility of conversations on tape-recordings. The court held that the recordings could be used as evidence provided, they were in accordance with certain requirements, including authentication, a flawless chain of custody, and corroboration by the other physical evidence. The ruling underlined the importance of ensuring digital evidence is not tampered with. This decision set the foundation for the later recognition of electronic evidence under section 65B of the Indian Evidence Act, 1872, which has now been replaced by section 63 of the Bharatiya Sakshya Adhiniyam, 2023. In *SIL Import, USA v Exim Aides Silk Importers*[48], the Supreme Court emphasised that the judicial interpretation of statutes must adapt to evolving technological contexts. The Court observed that laws should not be applied rigidly but must be construed in light of contemporary advancements to remain effective and relevant. This approach also ensures that legislative intent is preserved while the accommodating the realities of modern developments, particularly in areas influenced by rapid technological change.

The next milestone was *Anvar P.V. v P.K. Basheer*[49], which unequivocally enunciated the necessity of the certification of electronic records under section 65B.[50] The Supreme Court ruled categorically that secondary electronic evidence such as emails, SMS reports, and digital transactions could only be admitted in case of proof by a certificate under section 65B (4)[51] in order to establish authenticity and prevent tampering. This ruling reversed the earlier ruling in *State (NCT of Delhi) v Navjot Sandhu*[52], where oral evidence had been allowed to supplement electronic records.[53] The *Anvar P.V.* judgment is one of the milestone judgments on India's admissibility of digital evidence.

A shift towards a liberal approach, by the Court, was witnessed in *Shafhi Mohammad v State of Himachal Pradesh*[54], wherein the Supreme Court relaxed the condition of mandatory certification in cases where the party presenting electronic evidence did not possess the device from which the evidence was generated. This ruling was construed as an attempt to bridge the gap between procedural strictness and real difficulties faced by litigants in placing certified electronic records before the court. However, this relaxation itself was explained in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*[55], when the Supreme Court reaffirmed the necessity of certification under section 65B, except for circumstances where the original electronic device was produced in court.

Besides procedural admissibility, privacy and due process in online searches were at the centre of attention in *Justice K.S. Puttaswamy (Retd.) v Union of India*[56], where the Supreme Court declared the Right to Privacy to be a basic fundamental right within the contours of article 21 of the Constitution. The judgment stressed that surveillance by the States and digital search and seizure have to meet tests of necessity, proportionality, and reasonableness. The case directly influences law enforcement bodies conducting digital investigation since they have to ensure the seizure of electronic evidence does not violate any fundamental and constitutional rights, amongst the statutory ones. The right to privacy propounded as a cornerstone of search and seizure jurisprudence in India now acts as a fulcrum upon which the right of the State to conduct investigation and the right of the accused in terms of privacy rests to be balanced by the Courts.

The principle of *Doctrine of Forgone Conclusion* is widely debated in cases involving compelled decryption of electronic devices. In India, the right against self-incrimination enshrined under

[47] AIR 1986 SC 3.
[48] (1999) 4 SCC 567.
[49] (2014) 10 SCC 473.
[50] Indian Evidence Act 1872 (01 of 1872), s. 65B.
[51] Indian Evidence Act 1872 (01 of 1872), s. 65B (4).
[52] (2005) 11 SCC 600.
[53] Divyansha Goswami, 'Electronic Evidence in Focus: Navigating Legal Shifts in the Law on Electronic Evidence under the BSA, 2023' (SCC Online, 23 October 2024) <https://www.scconline.com/blog/post/2024/10/23/electronic-evidence-in-focus-navigating-legal-shifts-in-the-law-on-electronic-evidence-under-the-bsa-2023/> accessed 05 April 2025.
[54] (2018) 2 SCC 801.
[55] (2020) 7 SCC 1.
[56] *KS Puttaswamy* (n 38).

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

article 20(3) of the Constitution was reinforced in *Selvi v State of Karnataka*[57], where the Supreme Court ruled against compulsory brain mapping and narco-analysis. More recently, in *Virendra Khanna v State of Karnataka*[58], the Karnataka High Court held that law enforcement cannot force an accused to disclose passwords or decrypt devices without proper legal authorisation in the name of cooperating with the agencies conducting the investigation. *Per contra* the High Court of Delhi in *Sanket Bhadresh Modi v CBI*[59] held that even an accused, like the applicant, cannot be compelled to disclose passwords or comply with investigative expectations, as article 20(3) of the Constitution protects against self-incrimination as it enjoys an exalted status[60], especially during an ongoing trial. It is noteworthy that here the Delhi High Court even ruled out the possibility of legal authorisations in such instances. The courts while dealing with digital evidence must be mindful of the dictum laid down in *Kajal Sen*[61] case, by the Apex Court, regarding it is a duty of the (trial) court to appreciate evidence minutely, carefully, and to analyse it, as this forms the core of appreciation of evidence leading to proving or disproving of fact. Furthering this interpretation in the case of *Tukaram S. Dighole v Manikrao Shivaji Kokate*[62], Supreme Court ruled that standard of proof in the form of electronic evidence should be more accurate and stringent in comparison with other documentary evidence. In *Tomaso Bruno v State of Uttar Pradesh*[63], Supreme Court, upholding the trial court's view, held that failure to collect and produce critical electronic evidence—such as CCTV footage, call records, and SIM details of mobile phones seized from the accused—cannot be dismissed as mere lapses in investigation. Instead, such omissions constitute withholding of the best possible evidence, thereby undermining the prosecution's case. The Court emphasised that when the availability of such electronic records is not disputed and there is no justification for their non-production, it adversely affects the credibility of the investigation. This judgment underscores the vital role of digital evidence in modern criminal trials and affirms the legal expectation that investigating agencies must preserve and present all relevant electronic material, especially when it can decisively establish innocence or guilt. It also reinforces the judiciary's insistence on evidentiary completeness and procedural integrity in the digital era. In *Ram Ramaswamy v Union of India*[64], the Supreme Court's order of costs to the Union government for not responding to a plea for digital search guidelines, quietly mirrored the judiciary's increasing emphasis on executive inaction in safeguarding digital privacy.[65] Recently the Delhi High Court in *Rakesh Kumar Gupta*[66] has ordered the Customs Department to copy data from impounded electronic devices, like mobile phones, rather than keeping the physical devices in custody during legal proceedings. The move is designed to avoid loss of data due to device obsolescence and makes data easily accessible to investigators. The Court has indicated that once copies are made on media such as CDs or pen drives, with hash values to ensure data integrity, the original devices may be returned to their owners. This practice should be adopted in all Commissionerate to improve efficiency and minimize inconvenience to persons from whom devices are being confiscated. The ruling was made on a petition filed by persons whose mobile phones were confiscated by the Directorate of Revenue Intelligence under suspicion of participating in gold smuggling. The Court stated that unnecessary holding of devices during show cause notice proceedings or prosecutions could cause difficulty in recovery of data owing to technological development that makes devices obsolete.

Taken together, these decisions illustrate a moving worldwide and national direction toward strengthening judicial review, technological expertise, and legislative specificity in the case of digital evidence search and seizure. Growing reliance on digital forensics and electronic evidence in criminal

[57] *Selvi v State of Karnataka,* (2010) 7 SCC 263.
[58] 2021(3) AKR 455, 2021 KHC 11286.
[59] *Sanket Bhadresh Modi v CBI,* Bail Appl. 3754/2023, Crl. M.A. 1574/2023.
[60] *Santosh s/o Dwarkadas Fafat v State of Maharashtra,* (2017) 9 SCC 714; *Selvi v State of Karnataka,* (2010) 7 SCC 263.
[61] *Kajal Sen v State of Assam*, AIR 2002 SC 617.
[62] (2010) 4 SCC 329.
[63] (2015) 7 SCC 178.
[64] *Ram Ramaswamy and Ors. v Union of India,* WP (Crl.) 138/2021.
[65] Sohini Chowdhury, 'Supreme Court Imposes Rs. 25000 Cost on Centre for not Replying to Plea Seeking Guidelines for Seizure of Electronic Devices' (LiveLaw, 12 November 2022) <https://www.livelaw.in/top-stories/supreme-court-seizure-of-personal-electronic-devices-guidelines-plea-213964> accessed 05 April 2025.
[66] *Rakesh Kumar Gupta v Directorate of Revenue Intelligence (DRI)*, WP (C) 11518/2024.

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

trials necessitates a legal framework that balances state interests with the rights of citizens. While the Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023 introduce some procedural reforms, there are still challenges in cross-border digital investigations, encryption wall, and cloud-based evidence retrieval. There is a requirement for a robust National Cyber Forensic Policy, judicial sensitisation, and effective mechanisms to enforce compliance, to close such gaps. Finally, the development of case law on electronic evidence is to highlight the conflict between legal protection and technological advancement. Indian law has moved from strict procedural norms to a more subtle balance, protecting constitutional rights and the integrity of electronic evidence. As cyber-crimes are changing and evolving, the law relating to search, seizure, and forensic incorporation needs to be revised from time to time so that the dual purposes of efficient law enforcement and protection of the fundamental rights are met.

INTERNATIONAL BEST PRACTICES AND LESSONS FOR INDIA

Global best practices in search and seizure of electronic evidence stress the preservation of integrity, authenticity, and admissibility of digital information during the course of investigation and even after that. These practices include adhering to guidelines such as the ISO/IEC 27037:2012[67], which outlines procedures for identifying, collecting, acquiring, and preserving electronic evidence. Organisations like INTERPOL[68] and UNODC[69] recommend securing the crime scene, preserving chain of custody, and utilising authorised forensic equipment for avoiding data modifications. Moreover, the live acquisition technologies are utilised whenever systems cannot be shut down so that the volatile information is collected while critical infrastructure isn't interrupted. Furthermore, judicial supervision as well as the privacy protection is also a part of these practices that balance investigative necessities with personal privacy. Thus, through the use of these standards, law enforcement agencies (LEAs) around the globe can assure the validity of electronic evidence during legal trials.[70]

A) US Electronic Communications Privacy Act, 1986 (ECPA)

The Electronic Communications Privacy Act (ECPA) of 1986[71] is a pivotal U.S. legislation that has expanded the scope of privacy protections to include electronic communications. It was enacted to address the evolving technological landscape in US and also ensures that individuals' communications are safeguarded against unauthorised interception and access. The ECPA[72] is particularly relevant in the context of the search and seizure of electronic evidence, as it establishes legal norms for accessing electronic data while balancing privacy rights and law enforcement needs.

The ECPA[73] provides a comprehensive framework for law enforcement to access electronic evidence while ensuring that individuals' privacy rights are respected as guided by the First Amendment of the US Constitution. It also focuses on judicial oversight and procedural protections, like insisting on special warrants or court orders for searching certain categories of data. Nevertheless, the Act has been mostly criticised for neglecting entirely the latest in modern technological innovation, including cloud computing and encrypted communication in today's age.

In the current context, the ECPA[74] serves as the benchmark for analysing how the U.S. balances privacy rights with investigative needs. Its highlighting provisions can be contrasted with India's legal system, pointing out the various gaps that currently exist and the scope for improvement in Indian laws related to

[67] ISO/IEC 27037:2012 <https://www.iso.org/standard/44381.html> accessed 07 April 2025.

[68] INTERPOL, Cybercrime Threat Response <https://www.interpol.int/Crimes/Cybercrime/Cybercrime-threat-response> accessed 07 April 2025.

[69] UNODC, Standards and Best Practices for Digital Forensics <https://www.unodc.org/e4j/data/> accessed 07 April 2025.

[70] NIST Interagency Report NIST IR 8387, Digital Evidence Preservation <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf> accessed 07 April 2025.

[71] Electronic Communications Privacy Act, 1986 (US) Pub L No 99-508, 100 Stat 1848<https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285> accessed 07 April 2025.

[72] ibid.

[73] ibid.

[74]Electronic Communications Privacy Act, 1986 (US) Pub L No 99-508, 100 Stat 1848<.https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285> accessed 08 April 2025.

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

electronic evidence. The ECPA's focuses on judicial supervision and privacy safeguards provides useful lessons for formulating detailed guidelines in India.

B) UK's Investigatory Powers Act, 2016

The Investigatory Powers Act, 2016 (IPA)[75], often referred to as the "Snoopers' Charter", is a comprehensive legislation of UK, that governs the interception, acquisition, and retention of communications and data by the law enforcement and intelligence agencies. It brings together and modernises current surveillance powers to meet the challenges of twenty-first-century technology, making the investigative powers suitable for the digital era while adding mechanisms to safeguard the personal rights of the citizens.

The IPA[76] also provides a robust framework for balancing law enforcement needs with privacy rights, making it a valuable point of comparison for India's legal framework on electronic evidence. Its emphasis on judicial oversight, data retention policies, and safeguards for sensitive information offers insights into how India can address similar challenges. Hence, the authorities can by analysing the IPA[77], the highlight of the legislation is the importance of comprehensive legislation that adapts dynamically to technological advancements while protecting individual rights.

C) Comparative analysis in light of US, UK, and EU Cybersecurity laws

The legal frameworks governing cybersecurity in the United States, United Kingdom, and European Union embodies various distinct approaches which are influenced by their particular socio-political environments and technological settings. These laws are pertinent to prevent cyber threats and guarantee the integrity of the electronic evidence when conducting search and seizure activities.

4.3.1 United States Perspective

The U.S. cybersecurity landscape is characterised by a fragmented approach, with multiple federal and state laws addressing specific aspects of cybersecurity. Another one of the major legislation in this domain includes the Computer Fraud and Abuse Act (CFAA)[78], which criminalises unauthorised access to the computers, and the Electronic Communications Privacy Act (ECPA)[79], which protects the electronic communications from unauthorised interception by an attacker.[80] While these existing laws provide robust protections, the absence of a unified federal framework poses challenges for consistency across jurisdictions. The U.S. also emphasises judicial oversight, requiring warrants based on probable cause for accessing electronic evidence, as mandated by the Fourth Amendment of the United States Constitution. However, the rapid evolution of technology often outpaces legislative updates, leaving gaps in addressing emerging threats like cloud computing and encrypted communications between organisations.

4.3.2 United Kingdom Perspective

The UK has adopted a more consolidated approach to cybersecurity through legislation like the Investigatory Powers Act, 2016 (IPA) and the upcoming Cyber Security and Resilience Bill, 2024.[81] The IPA governs the interception, acquisition, and retention of communications, emphasizing judicial oversight and privacy safeguards. The Cyber Security and Resilience Bill aims to fortify critical infrastructure and digital services against escalating cyber threats, introducing stricter incident reporting requirements and supply chain security measures.[82] The UK's focus on adapting its laws to address technological advancements ensures a proactive stance in combating cybercrime. However, balancing national security interests with individual privacy rights remains a challenge before the state.[83]

4.3.3 European Union Perspective

The EU's cybersecurity framework is harmonised across member states, ensuring a

[75]Investigatory Powers Act 2016 (UK) c 25 <https://www.legislation.gov.uk/ukpga/2016/25/contents> accessed 08 April 2025.

[76]ibid.

[77]ibid.

[78] Computer Fraud and Abuse Act, 1986 (US) 18 USC, s. 1030.

[79] Electronic Communications Privacy Act, 1986 (US) Pub L No 99-508, 100 Stat 1848.

[80] 'Cybersecurity Laws and Regulations, 2025' <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa> accessed 08 April 2025.

[81]'UK's New Cybersecurity Bill threatens £100K fines' <https://www.computing.co.uk/news/2025/legislation-regulation/uk-cybersecurity-bill-threatens-100k-daily-fines> accessed 08 April 2025.

[82]'UK Government sets out scope for Cyber Security and Resilience Bill'<https://natlawreview.com/article/uk-government-sets-out-scope-cyber-security-and-resilience-bill#google_vignette> accessed 08 April 2025.

[83] 'Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation' <https://www.congress.gov/crs-product/R42114> accessed on 08 April 2025.

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

high level of protection through regulations like the Cybersecurity Act, 2024[84] and the NIS2 Directive, 2020.[85] The Cybersecurity Act strengthens the mandate of ENISA, the EU Agency for Cybersecurity, and establishes a certification framework for ICT products and services.[86] The NIS2 Directive enhances cross-border cooperation and imposes stricter requirements on critical infrastructure operators. The EU's emphasis on collaboration and standardization ensures consistency in addressing cyber threats while promoting trust and resilience. However, the implementation of these regulations across diverse member states can be complex and resource-intensive.

D) ISO/IEC 27037:2012 Standard and Cyber Forensics

The ISO/IEC 27037:2012[87] (Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence) standard provides comprehensive guidelines for the identification, collection, acquisition, and preservation of digital evidence. It is a benchmark for guaranteeing the admissibility and integrity of electronic evidence in legal proceedings and disciplinary procedures. The standard is most directly applicable to the context of search and seizure actions by the law enforcement agencies, where it provides guidelines on how the digital evidence should be collected and processed with its evidential value preserved.

The principles outlined in ISO/IEC 27037:2012[88] are highly relevant to search and seizure operations involving electronic evidence. Hence, when following these standards, law enforcement agencies (LEAs) can guarantee that the digital evidence is processed in a way that preserves its admissibility in court of law. The standard also covers various important challenges like data encryption, remote storage, and cloud service usage, which are increasingly prevalent in contemporary investigations.

ISO/IEC 27037:2012[89] is recognised internationally as a benchmark for handling digital evidence. Its core principles can be adapted to suit the local legal and the technological contexts of different jurisdictions. For example, India can integrate these guidelines into their laws to overcome loopholes and grey areas in the search and seizure of digital evidence to provide the consistency and reliability in digital investigations. Its focus on best practices, accountability, and technological responsiveness makes it a necessity for contemporary investigations. The integration of this standard into national legal frameworks that is yet to be drawn, our country can enhance their capacity to handle electronic evidence effectively, fostering trust in their judicial systems, while working with the LEAs at the same time.

E) Key Takeaways for India

The above comparative analysis highlights the importance of adopting a comprehensive and adaptive cybersecurity framework. As of now, Indian State can draw lessons from the U.S. emphasis on judicial oversight which is of imminent need, the UK's focus on incident reporting and supply chain security, and the EU's harmonised approach to cross-border collaboration makes it a dire need of today. The integration of these elements into its legal framework, our country can address the challenges of search and seizure of electronic evidence while safeguarding individual rights and ensuring the integrity of digital investigations as these will be pertinent in the future. Current practices followed in India face numerous challenges, including technological complexities, jurisdictional ambiguities, privacy concerns, and skill gaps among law enforcement personnel where Telangana Police's Standard Operating Procedures[90] (SOP) for New Criminal Laws shed light on the day to day procedure to be followed as guided by the SOPs formulated by the state police regarding search and seizure protocol from a technical forensic perspective as enumerated to be followed by the law enforcement agencies of the state, and on

[84] EU Cybersecurity Act 2019 <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act> accessed on 09 April 2025.

[85] 'What is the NIS2 Directive?' <https://nis2directive.eu/what-is-nis2/> accessed on 09 April 2025.

[86] *EU Cybersecurity Act* (n 83).

[87] ISO/IEC 27037:2012 <https://www.iso.org/standard/44381.html> accessed 09 April 2025.

[88] ibid.

[89] ibid.

[90] Bureau of Police Research and Development, 'Standard Operating Procedures for New Criminal Laws' Telangana Police (BPR&D) <https://bprd.nic.in/uploads/pdf/Standard_Operating_Procedures.pdf> accessed 10 April 2025.

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

the other side CBDT Digital Evidence Investigation Manual[91] for Tax authorities provides a sigh of relief for the citizens as a check on search procedures by the taxation authorities, whereas similarly in the far north-eastern region of India where accessibility to resources are minimum, SOPs of Tripura Police[92] can be seen a ray of light at the end of a long dark tunnel where the two rails of privacy and law enforcement never meet each other.

CONCLUSION AND SUGGESTIONS

A) Proposed National Framework for Cyber Forensic and Digital Evidence

To address the challenges associated with the search and seizure of electronic evidence, a robust *National Framework for Cyber Forensic and Digital Evidence* should be established, as it is *sine qua non,* for issues highlighted herein in this age and era of technological advancements. This framework would ensure the integrity, authenticity, and admissibility of digital evidence while balancing investigative needs with individual rights. The organisational flow of the proposed framework:

5.1.1 Comprehensive Legal Guidelines:

Formulating a comprehensive legal framework that embodies provisions of current laws like the Information Technology Act, 2000 and the Bhartiya Sakshya Adhiniyam, 2023 as well as details on search, seizure, preservation, and admissibility of electronic evidence in a Court of law at trial stage.

5.1.2 Cyber Forensic Standards:

Embracing and conforming to global standards such as ISO/IEC 27037:2012 for the identification, collection, acquisition, and preservation of digital evidence. The recent legal requirement for the employment of certified forensic tools and methods to guarantee the quality of evidence has been a move in the right direction concerning digital evidence collection and preservation under the Bharatiya Nyaya Suraksha Sanhita, 2023.

5.1.3 Specialised Cyber Forensic Units:

Setting up specialised and dedicated cyber forensic units in law enforcement agencies with the latest tools and technologies. These units must specialize in retrieving encrypted data, examining cloud-based evidence, and dealing with cross-border digital investigations.

5.1.4 Training and Capacity Building:

Making provision for regular training courses for law enforcement officers, forensic specialists, and members of the judiciary to deepen their knowledge on digital evidence on a regular basis, so as to keep them abreast of the latest developments happening in the domain. Additionally, creating various specialized courses on upcoming technologies, including blockchain and artificial intelligence, to prepare for future challenges.

5.1.5 Chain of Custody Protocols:

Introducing standardised procedures for documenting the chain of custody (for e.g., using Faraday Bag[93] to collect hard drives) to maintain the integrity of digital evidence. Ensure that all actions taken during the investigation are recorded and verifiable.

5.1.6 Privacy and Data Protection Safeguards:

Incorporating privacy safeguards to prevent misuse of personal data during investigations and aligning the framework with data protection laws, such as the Digital Personal Data Protection Act, 2023[94], to uphold individual rights.

5.1.7 Judicial Oversight and Accountability:

Establishing mechanisms for judicial oversight to ensure that search and seizure operations comply with legal and ethical standards. In addition to it, introducing accountability measures to prevent abuse of power by law enforcement agencies.

5.1.8 Cross-Border Collaboration:

Strengthening international cooperation through mutual legal assistance treaties (MLATs) and agreements to address jurisdictional challenges in accessing electronic evidence stored overseas and at the same time also collaborating with global organisations like INTERPOL for first responders[95] and global guidelines[96] and UNODC guidelines on cross

[91] *CBDT Manual* (n 21).

[92] Tripura Police Training Academy, 'Standard Operating Procedures for Dealing Cases under Various Special Acts' (Tripura Police, February 2024) <https://police.tripura.gov.in/sites/default/files/2024-02/SOPs_of_PTA_0.pdf> accessed 10 April 2025.

[93] 'Faraday Bags are the First Step in Preserving Digital Evidence' (MOS Equipment, 6 April 2023) <https://mosequipment.com/blogs/blog/faraday-bags-are-the-first-step-in-preserving-digital-evidence> accessed 10 April 2025.

[94] *DPDP* (n 42).

[95] INTERPOL, Guidelines for Digital Forensics First Responders (INTERPOL 2022) <https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf> accessed 10 April 2025.

[96] INTERPOL, *Global Guidelines for Digital Forensics Laboratories* (INTERPOL 2021) <https://www.interpol.int/en/content/download/13

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

border evidence collection[97], besides standards and best practices for evidence collection[98] to adopt best practices.

5.1.9 Research and Development:

Investing in research to develop indigenous forensic tools and technologies tailored to India's unique requirements. While at the same time encourage public-private partnerships to foster innovation in the field of cyber forensics.

5.1.10 Public Awareness and Education:

Launching awareness campaigns to educate citizens about their rights and responsibilities concerning digital evidence and also promoting ethical practices in the handling and use of electronic evidence.

The above proposed framework by the researchers aims to create a standardised and efficient system for managing cyber forensic and digital evidence, ensuring that investigations are conducted transparently and effectively while safeguarding individual rights.

B) The way forward

In conclusion, the establishment of a National Framework for Cyber Forensic and Digital Evidence is an earnest requirement nowadays, as technology and crime are connecting each other in more complex manners. The proposed framework here strives to address multi-dimensional problems involved in searching, seizing, keeping safe, and admitting electronic evidence within the overall milieu of India's developing legal regime. By offsetting provisions in statute under legislation such as the Information Technology Act, 2000, Bharatiya Sakshya Adhiniyam, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023, and aligning these with international standards and best practice, the framework aims to create a harmonious and constitutionally sound digital evidence system. This proposal pivots around the integration of technologically advanced forensic processes, capacity development for all stakeholders, and judicial oversight mechanisms to ensure due process and avoid abuse. Here, equally important is the appeal for focus on data security habits and privacy defences conventions in accordance with the Digital Personal Data Protection Act, 2023. The above proposed strategy also emphasises the importance of enhancing international coordination in addressing various jurisdictional impediments associated with cross-border cybercrimes as well as rationalising India's practices in accordance with international paradigms such as those presented by INTERPOL and the UNODC. Moreover, sustained investment in research and development, as well as the public-private collaborations, will make India not only adaptive to changing threats but also independent in forensic innovation. Furthermore, public awareness campaigns and education initiatives will further democratise the digital evidence discussion, enabling an educated citizenry. Collectively, this strategy seeks to address the twin challenges of good law enforcement and the preservation of basic rights in the age of the Internet, thereby creating an effective and technology-informed but constitution-obedient system of justice.

501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf> accessed 10 April 2025.

[97] UNODC, *Practical Guide for Requesting Electronic Evidence Across Borders* (UNODC 2019) <https://www.unodc.org/unodc/en/terrorism/expertise/electronic-evidence.html> accessed 10 April 2025.

[98] UNODC, *Standards and Best Practices for Digital Forensics* (UNODC 2020) <https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html> accessed 10 April 2025.