AN ANALYSIS OF DIGITAL SEARCH AND SEIZURE UNDER INDIAN CRIMINAL LAW

Muskan Yadav* **Ayush Rajpoot***

ABSTRACT

The emergence of the digital technology has rapidly changed the manner in which the act of maintaining the law enforcement investigations are carried out. In the present legal context, electronic devices such as laptops, computers, mobile phones, cloud storage solutions, and social media platforms act as important evidence sources. However, India's laws related to search and seizure were originally designed for tangible evidence and often struggle to address the unique problems presented by digital information. This study methodically assesses the relevance of the search and seizure regulations in the 1973 Code of Criminal Procedure regarding digital evidence. The study evaluates the legal frameworks, constitutional safeguards, and judicial interpretations linked to digital privacy, electronic searches, and the levels of evidence. The research pointed out the important procedural gaps and argues that particular legal safeguards are necessary to regulate digital queries. To ensure a successful balance between criminal investigation and protection of fundamental rights in the digital era, the text proposes measures.

Keywords: Digital Evidence, Search and Seizure, Privacy, Cyber Law, Electronic Records.

RESEARCH METHODOLOGY

The research approach used in this study is doctrinal. The investigation involves primary legal sources (binding authority) and secondary legal sources (non-binding authority), building the foundational framework for research. The Indian Constitution, the Information Technology Act of 2000, the Code of Criminal Procedure of 1973, and rulings from the Supreme Court and other High Courts are examples of primary sources. Books, journal articles, legal commentary,

*BA LLB (HONS.), THIRD YEAR, MARWADI UNIVERSITY, RAJKOT.
*BA LLB (HONS.), THIRD YEAR, MARWADI UNIVERSITY, RAJKOT.

reports, and academic publications about criminal process and digital evidence are examples of secondary sources. Alongside recognising deficiencies in existing laws and administrative procedures, the research aims to critically assess the sufficiency of contemporary legal provisions.

LIMITATIONS OF THE STUDY

The inquiry into legal acts, court judgments, legal sayings, scholarly works, and official reports of the government forms the basis of this research, which is fundamentally doctrinal in character. Other methods like surveys, interviews, or field work, or inquiries involving law enforcement, forensic specialists, or judges are not used in this study.

This research is not carried out through the technical analysis of digital forensic procedures and is limited to the legal framework authorising digital search and seizure under the Indian criminal law. Also, the study is restricted to publicly accessible legal and scholarly sources due to the restrictions on access to sensitive investigative documents and enforcement organisations' operating processes.

This study mainly focuses on judicial interpretations, legislative provisions, constitutional protections, and the procedural problems related to digital evidence and electronic searches in the Indian legal system.

OBJECTIVES OF THE STUDY

1. To examine the legal framework governing search and seizure under Indian criminal law.
2. To analyse the role of digital evidence in modern criminal investigations.
3. To study constitutional safeguards relating to digital searches.
4. To identify loopholes and procedural gaps in the existing framework.
5. To suggest reforms for regulating digital search and seizure.

RESEARCH QUESTIONS

1. Do the existing provisions relating to search and seizure adequately regulate digital evidence?
2. What constitutional safeguards govern digital searches and seizures?
3. What challenges arise in the collection and preservation of digital evidence?

4. What reforms are necessary to modernise criminal procedure in relation to digital investigations?

INTRODUCTION

The quick development of technology has changed the nature of criminal investigation.[1] Large volumes of electronic data have been produced as a result of the increasing use of computers, cellphones, social media sites, and cloud-based services. In criminal cases, this kind of material is sometimes used as critical evidence. To increasement of these uses, law enforcement organisations are depending more and more on digital evidence to investigate and prosecute crimes.

The time when the majority of evidence was tangible. The Code of Criminal Procedure, 1973, created the traditional search and seizure rules. With the rise of digital evidence, significant difficulties with this approach have been shown. Electronic data may be copied, changed, encrypted, remotely erased, and kept across several countries, unlike physical items.[2]

These traits call for specific procedural protections, including the recognition of privacy as a basic right under Article 21[3] of the Indian Constitution, and further underscore the necessity to properly control digital searches. Electronic devices hold extremely private information unrelated to the crime being investigated. As a result, uncontrolled access to these gadgets poses major privacy and individual liberty issues. The necessity for a modern legal framework that can protect constitutional rights and handle modern investigation difficulties. Along with the importance of digital evidence is also discussed in this chapter.

CONCEPT AND LEGAL FRAMEWORK OF SEARCH AND SEIZURE UNDER CRPC

To verify a crime, searching and seizing play a big role when officials look into criminal conduct; officials can collect proof related to crimes. The rules that cover how these actions must happen sit inside the Code of Criminal Procedure from 1973.[4]

[1] Justice Yatindra Singh, Cyber Laws (Universal Law Publishing 2021).< https://store.lexisnexis.com/en-in/products/cyber-laws-insku9789351437338.html>
[2]Aparna Viswanathan, Cyber Law: Indian and International Perspectives (LexisNexis 2012).
< http://advocatesstore.in/index.php?route=product/product&product_id=487>
[3] K.S. Puttaswamy v Union of India (2017) 10 SCC 1.
[4] Code of Criminal Procedure 1973, ss 91, 93, 100 and 102.

Investigating areas aims to find proof that people might hide, demolish, or keep out of reach. Still, these actions hit the personal space and freedom hard. The Procedures exist so that the power isn't used carelessly - rules step in to hold things together.

Starts with a point made by K.N. Chandrasekharan Pillai in R.V. Kelkar's Criminal Procedure: search and seizure powers go against normal personal freedom, yet still need exact legal follow-through.[5] Even if these acts need full coordination with rules, they avoid the standard rights. Because liberty is central, and any break from it demands accurate conditions. When deviation happens, the procedure becomes essential. Not every power fits flexibly within justice; some misinterpret the core principles, but they are strictly controlled. So long as such tools exist, compliance holds more weight than the intended.

Although some regulations allow searches without warrants, judicial authorisation is required. Only during an emergency do officers skip that step. When property gets taken, someone has to write down what happened. Reasons for taking items must be put on paper. Clear steps keep the process open to review.

Back when these rules started, they dealt only with physical items. Still, their wording stretches far enough to include gadgets like phones and computers. Because of that stretch, applying them online gets tricky pretty fast. Even though it gives power to monitor, collect, and keep data, the Information Technology Act, 2000 recognises digital records within the justice process.[6] Yet a complete set of rules for online search and seizure still doesn't exist under its scope.

SEARCH AND SEIZURE UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023

With the passage of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), which replaced the Code of Criminal Procedure, 1973, India's criminal procedural framework has recently experienced significant modification.[7] Through increases in the use of technology and electronic communication within procedural procedures, the BNSS aims to modernise criminal investigations.

[5] K.N. Chandrasekharan Pillai, R.V. Kelkar's Criminal Procedure (Eastern Book Company 2023).
[6] Information Technology Act 2000.
<https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf>
[7] Bharatiya Nagarik Suraksha Sanhita 2023.

In a number of BNSS requirements, the increasing importance of digital communication and electronic records in criminal proceedings is acknowledged. The law also promotes the use of technology in evidence management, documentation, and inquiry. These developments are especially relevant in the framework of digital search and seizure, as data held in electronic devices and internet platforms is becoming more and more significant in modern investigations.

The BNSS does not, however, create a comprehensive set of rules that directly control digital searches, electronic warrants, forensic data collection, or limitations on access to personal digital information, while introducing technical advancements. As a result of this context, the new framework still faces many of the same difficulties as the Code of Criminal Procedure. So begins a new chapter where the move from CrPC to BNSS reveals advances, yet gaps remain in how digital probes are handled. Though tools improve, old weaknesses linger behind fresh rules. Not everything changes just because names do. Some parts work better now; still others drag along unchanged. Progress appears, but not everywhere at once. What was fixed might still bend under pressure. Even with updates, certain problems refuse to fade away.

Even though updates to procedures have started, specific safeguards must remain in place when searching electronics. These rules protect individual rights under the Constitution. They also help make sure any evidence collected stays trustworthy. Without them, fairness could be at risk. Modern methods do not remove that need.

DIGITAL EVIDENCE AND CONTEMPORARY CRIMINAL INVESTIGATIONS

Data kept or sent electronically that might be applied in court is referred to as "digital evidence." Because of the frequent use of digital technology, such evidence has grown in importance in criminal investigations.

Emails, texts, call logs, social media posts, CCTV video, computer files, and cloud-based data are examples of common digital evidence. Digital evidence commonly offers insightful data about the behaviour, motivations, and acts of the suspects.[8]

The digital information is much more fragile and vulnerable to manipulation than tangible proof. As a result, investigators need to follow certain protocols for gathering, storing,

[8] Tomaso Bruno v State of Uttar Pradesh (2015) 7 SCC 178.

analysing, and presenting the information. Legality may be challenged in court if the integrity of the evidence is compromised.[9]

Identification, preservation, collection, inspection, analysis, and presentation are ordinary steps in the management of digital evidence. Technical know-how and adherence to forensic standards are necessary at each point. The digital investigations are made more problematic by issues like encryption, password security, cloud computing, and cross-border data storage. As an outcome, both technological proficiency and legislative protections are necessary for present criminal investigations.

ELECTRONIC EVIDENCE AND THE BHARATIYA SAKSHYA ADHINIYAM, 2023

The admissibility of digital evidence is one of the most important parts of contemporary criminal investigations. And electronic device seizures are only significant when the data they produce can be acknowledged and used as evidence in court.

The Indian Evidence Act, 1872 has been replaced by the Bharatiya Sakshya Adhiniyam, 2023, which also consists of rules related to digital and electronic documents. The Act aims to include technology advancements into the proof that is based on norms and recognise the electronic data as documented evidence.[10]

Emails, texts, social media posts, computer files, CCTV footage, metadata, server logs, and data kept in the cloud are examples of digital evidence. And the electronic records are liable to change, duplication, and deletion, in contrast to conventional documented proof. Consequently, to guarantee validity and reliability, procedural precautions are essential.

Electronic evidence must comply with the legal standards for validity and certification to be admitted.[11] The significance of upholding the procedural protections to deter interference and ensure proof-based integrity has been repeatedly emphasised in court rulings.

In the context of this, the Bharatiya Sakshya Adhiniyam is essential in controlling the admissibility of digital data obtained by search and seizure procedures. In the end, the efficacy

[9] National Judicial Academy, Electronic Evidence and Cybercrime Investigation (NJA Publication 2020).
[10] Bharatiya Sakshya Adhiniyam 2023.
[11] Anvar PV v PK Basheer (2014) 10 SCC 473.

of digital investigations relies not only on the legitimacy and admissibility of electronic evidence in court but also on legal gathering.

PRIVACY JURISPRUDENCE AND JUDICIAL INTERPRETATION

The discussions on digital search and seizure frequently revolve around privacy issues. Such as financial records, private messages, medical information, and photos are just a few of the many pieces of personal data that are stored on electronic devices. Accessing such data without sufficient security measures might lead to serious privacy breaches. Privacy was recognised as a basic right safeguarded by Article 21 of the Indian Constitution in the historic ruling in the case of K.S. Puttaswamy v. Union of India.[12] In this ruling, according to the Supreme Court, any invasion of privacy must comply with the requirements of need, proportionality, and legality.

SELF-INCRIMINATION AND DEVICE ACCESS

Under Article 20(3) of the Indian Constitution, which shields people from self-incrimination, raises another fundamental issue. Significant legal concerns about forced access to electronic data have been raised by the increase in the usage of smartphones and encrypted digital gadgets.

During criminal investigations, investigating authorities often come with password-protected gadgets. So, the question of whether an accused individual may be forced to provide passwords, unlock devices, or grant biometric access like fingerprints or face recognition emerges.

The Supreme Court in Selvi v State of Karnataka held that testimonial coercion is covered under the constitutional provisions against self-incrimination.[13] Not specifically analysing smartphone encryption, the ruling's guiding principles are very crucial for figuring out whether the forced access to digital devices is lawful or unlawful. The Indian criminal process faces ambiguity due to the absence of explicit law regulations permitting the compulsion of handwriting samples. To strike a balance between the investigative interests and the constitutional protections against self-incrimination, further legislative reform may be required. The Court emphasised that one crucial component of individual freedom is

[12] K.S. Puttaswamy v Union of India (2017) 10 SCC 1.
[13] Selvi v State of Karnataka (2010) 7 SCC 263.

informational privacy. Since sensitive personal data is often accessed through electronic searches, this concept has important consequences for digital investigations.

Through the ruling of the courts, the law pertaining to electronic evidence has been changed. The Supreme Court emphasised the significance of legislative compliance with regard to electronic documents in the case of Anvar P.V. v. P.K. Basheer. In the case of Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal later confirmed the need for procedural protections to guarantee authenticity and dependability.

COMPARATIVE LEGAL FRAMEWORK

In several states, the specialised legal frameworks governing digital search and seizure have been implemented.

In most of the cases, law enforcement officials must have warrants before accessing any digital devices due to constitutional safeguards against unreasonable searches in the United States.[14] Also, judicial supervision guarantees that searches are reasonable and specific. In a similar vein, the UK has also passed laws governing digital information access and electronic monitoring. Data protection and informational privacy are highly valued in European states.

India still mainly depends on customary procedural rules and court interpretation, in contrast to these nations. Uncertainty and inconsistency result from the lack of a specific legal framework for digital searches.

According to a comparative study, India would gain by enacting specific laws that deal with digital evidence, privacy rights, and procedural protections.

INTERNATIONAL COOPERATION AND BUDAPEST

Convention: The cross-border access to electronic evidence is one of the biggest impediments in digital investigations. Evidence collection is challenging and also time-consuming since criminal data is often kept on servers outside of national governments.

[14] Fourth Amendment to the United States Constitution.< https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-fourth-amendment-mean>

The Budapest Convention on Cybercrime is one of the most significant international agreements relating to cybercrime investigations and electronic evidence.[15] The Convention develops the procedures for requests for preservation, reciprocal legal aid, and international collaboration in the acquisition of digital evidence.

The Convention's principles offer helpful advice about cross-border evidence collection and procedural safeguards, even though India is not yet a party to it. The International cooperation frameworks will be crucial for successful criminal investigations as cybercrime increasingly crosses national borders.

The growing internationalisation of digital evidence, therefore, underscores the need for harmonised legal standards and efficient mechanisms for transnational evidence collection.

DIGITAL FORENSICS AND CHAIN OF CUSTODY

The methods that are used for collecting, storing, analysing, and presenting digital evidence have a significant impact on its dependability. In order to guarantee that electronic evidence is legitimate and unchanged, digital forensic science is essential.

The identification of electronic devices, information preservation, forensic data collection, digital content assessment, evidence analysis, and the creation of forensic reports are all typical steps in the digital forensics process. The investigators must make sure that the original data is not changed during this procedure.

The creation of forensic photographs of digital devices is a crucial security measure. An identical copy of an electronic storage medium made with a specialised tool is called a forensic image. Write-blocking technology is often used by investigators to avoid unintentional data alteration during the time of investigation. The hash values are used to confirm the integrity of digital evidence. Investigators and judges can verify that electronic data has not been tampered with after seizure thanks to hashing, which creates another digital fingerprint.[16]

The chain of custody is another important condition. The handling, transport, inspection, and storage of digital evidence should all be precisely recorded. Any type of possible breach in the chain of custody might raise suspicion about its legitimacy and dependability.

[15] Convention on Cybercrime (Budapest, 23 November 2001).
[16] National Judicial Academy, Electronic Evidence and Cybercrime Investigation (NJA Publication 2020).

Increases in the use of digital evidence highlight the need for specialised forensic labs, skilled staff, and consistent national guidelines for managing electronic evidence.

Finding gaps in procedures and loopholes: Even with laws in place about searches and seizures, problems still show how they are carried out. Procedures often fall short when put into practice.

Lack of Full Digital Search System: Back when these rules took shape, paper trails ruled the day. Now, probing data traces runs into snags the old framework never saw coming.

Lack of Digital Search Warrants: Right now, the rules don't spell out clear boundaries on how long digital search warrants last or what they cover. Details about their reach stay missing from existing legislation. What these warrants can touch remains loosely defined by law. Limits on access to electronic gadgets aren't laid out clearly anywhere. The legal framework skips specifics that would help shape such searches.

Absence of Data Extraction Limits: Should probes open doors to masses of private data beyond the crime being probed, unease grows. Privacy feels drawn-out and too feeble when the details with no link to the wrongdoing are still getting swept up.

Inadequate Chain of Custody Standards: Because the digital proofs require careful handling, every step must be recorded. Without clear rules that everyone follows, proof might lose its strength.

Cross-Border Data Storage Challenges: Some of the companies keep the data beyond the Indian borders, which slows things down when authorities need access to it. Getting the proof takes longer because of where the servers sit.

Encryption and Access Issues: Modern encryption technologies regularly hinder the authorisation to digital information, creating challenges for investigators.

Privacy Concerns: Broad search powers may reveal sensitive personal information irrelevant to criminal activity. Such intrusions may compromise constitutional protections.

Impact of the Digital Personal Data Protection Act, 2023: The Digital Personal Data Protection Act of 2023 is a significant recent development. The Digital Personal Data

Protection Act reflects the increasing awareness of informational privacy and provides a framework for the processing and protection of personal data in India.[17]

The Digital Personal Data Protection Act has a substantial bearing on digital search and seizure, even if the Act's main focus is on data processing operations. Extensive personal data, including bank records, conversations, medical information, and professional papers, is sometimes found on electronic devices seized during investigations. The Act does not fully control digital searches carried out during criminal investigations, even if it offers exceptions for law enforcement. Therefore, there is still a gap between criminal procedural law and data protection standards. This brings up how crucial it is to build something specific - something that weighs personal privacy against the demands of investigation while ensuring entry into digital data stays fair and secure.

RECOMMENDATIONS AND REFORM PROPOSALS

Out of today's tech challenges comes a need - laws must catch up. Electronic probes run wild without clear rules. Something new could fix that gap. A focused law on digital searches might just bring order. Instead of guessing, officers would follow set steps. Clarity often prevents misuse. This kind of act wouldn't invent justice - it'd reflect it.

Only a judge's approval ought to let authorities look at phones, laptops, online files, or similar gadgets - unless certain conditions apply. The nature, scope, duration, and categories of information that may be examined should be clearly specified through Digital warrants.

The data minimisation principles should be incorporated to ensure that the investigators access only information relevant to the offence under investigation. Uniform national standards should be established for forensic imaging, preservation of metadata, hash verification, and chain of custody documentation.

The specialised cyber-forensic laboratories should be expanded throughout the country. The investigating officers, prosecutors, and judicial officers should have regular training in digital evidence management. The mechanisms governing the cross-border access to electronic evidence should be enhanced through international cooperation agreements.

[17] Digital Personal Data Protection Act 2023.

Clear statutory provisions should regulate compelled decryption and access to encrypted devices. Privacy safeguards consistent with Article 21 of the Indian Constitution should be incorporated into all digital investigation procedures.

CONCLUSION

Digital evidence is becoming a very important part of modern criminal investigations. However, the legal system that controls search and seizure in India is still mainly based on concepts intended for tangible evidence. The development of digital technology has brought to light the important constitutional and procedural issues that are difficult for current legislation to adequately handle.

The demand to strictly regulate digital search powers has increased due to the recognition of privacy as a fundamental right. The insufficiency of the present structure is highlighted by the lack of defined guidelines controlling data extraction limitations, chain of custody norms, and digital warrants.

The review emphasised that to update criminal laws and guarantee conformity with technological progress, legislative change is required. Equitably balancing the investigation with constitutional protection would significantly enhance the administration of criminal justice in the digital age.

REFERENCES

1. Constitution of India, 1950.
2. Code of Criminal Procedure, 1973.
3. Information Technology Act, 2000.
4. Indian Evidence Act, 1872.
5. Digital Personal Data Protection Act, 2023.
6. Bharatiya Nagarik Suraksha Sanhita, 2023.
7. Bharatiya Nagarik Suraksha Sanhita, 2023.
8. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
9. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
10. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
11. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
12. Selvi v. State of Karnataka, (2010) 7 SCC 263.

13. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.
14. K.N. Chandrasekharan Pillai, *R.V. Kelkar's Criminal Procedure* (Eastern Book Company, Latest Edition).
15. V.N. Shukla, *Constitution of India* (Eastern Book Company, Latest Edition).
16. Aparna Viswanathan, *Cyber Law: Indian and International Perspectives* (LexisNexis).
17. Talwant Singh, *Cyber Law and Information Technology*.
18. Articles published in the *Indian Journal of Law and Technology*.
19. Articles relating to digital evidence, cybercrime investigations and privacy rights published in legal databases such as SCC Online, Manupatra and HeinOnline.
20. Law Commission of India Reports relating to Criminal Procedure and Electronic Evidence.
21. National Judicial Academy Publications on Electronic Evidence and Cybercrime Investigation.
22. Justice B.N. Srikrishna Committee Report on Data Protection.
23. Supreme Court of India Official Website.
24. Ministry of Electronics and Information Technology (MeitY) Official Publications.
25. Legislative Department, Government of India.
26. SCC Online Database.
27. Manupatra Legal Database.
28. HeinOnline Academic Database.
29. Indian Kanoon