International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(22s) 2026 pp. 349-361
https://doi.org/10.70917/ijcisim-2026-5435
Article

# Digital Forensics, Informational Privacy and Constitutional Dignity: A Critical Study of Cybercrime Investigative Framework under BNSS and DPDP Act

**Puneet Sharma[1*], Prof. Dr. Archana Sarma[2]**

[1]Phd Scholar, The North Cap University, Gurugram, Haryana-122017, email id puneetsharma1812@gmail.com
[2]HOD and Professor, The North Cap University, Gurugram, email id: archanasarma@ncuindia.edu.

**Abstract:** The rapid expansion of cybercrime investigation has brought fundamental changes in the manner in which criminal investigations are used to be conducted in India, especially with increased usage of digital forensic technologies during extraction, preservation, and analysis of electronic devices seized during cybercrime investigations. However, these modern digital forensic technologies help in increasing the technological capabilities of our law enforcement agencies. On the other hand, it also raises several constitutional concerns as well, such as breach of informational privacy, constitutional dignity, procedural fairness, and protection against self-incrimination guaranteed under Article 21 and 20(3) of the Indian Constitution, due to unrestricted extraction of personal information by investigative authorities. Therefore, it can be said that technological upgrades in criminal investigations have expanded faster than constitutional and procedural safeguards. This article attempts to evaluate critically India's legal and constitutional framework governing digital forensic investigations, with special focus on the investigation stage of cybercrime investigation. This article includes analysis of various constitutional provisions protecting the right to privacy, along with India's procedural framework regulating investigative data practices, forensic extraction, and state access to personal digital information, such as the Bharatiya Nagarik Suraksha Sanhita 2023 and the Digital Personal Data Protection Act, 2023. This article argues that though India's legal framework has been updated recently to accommodate electronic investigation within in its criminal procedure, but the absence of comprehensive statutory framework specifically regulating digital forensic governance, forensic laboratories, extraction limitation, electronic device search and seizure practices, protocols for cloning the device, data minimization requirement during cybercrime investigation has substantially impacted the dignity as well as fail to secure informational privacy of the suspect of an alleged offence.

**Keywords:** Digital forensic investigation, Informational Privacy, Constitutional Dignity, Data minimization, electronic devices.

## 1. INTRODUCTION

The rapid integration of technology in our social, communicative, and economic life is easily noticeable. Nowadays, criminals are using more advanced and sophisticated technologies in order to commit crimes. As a result, the nature of criminal investigation has also changed drastically. For instance, cloud infrastructure, metadata systems, encrypted communications, algorithmically generated content, and electronic devices are often used in cyber offences. Consequently, digital evidence like mobile phones, laptops, e-mails, metadata, CCTV footage, and cloud storage plays a central evidentiary role in contemporary criminal investigations. Therefore, law enforcement agencies in India are compelled to rethink traditional investigative practices and are moving toward adopting new technologies for detection, prevention, and investigation of cybercrimes.

Recently, cybercrime cases have been increasing at a rapid pace across the globe; India is also witnessing such a significant rise. More particularly, in India, we are witnessing such a surge in financial fraud cases that has resulted in a considerable number of economic losses. For instance, in the year 2023, a total of 86450 cybercrime cases were

registered across India, whereas only 65893 were registered in the year 2022. The 2023 report of the National Crime Record Bureau clearly demonstrates that cybercrime cases surged by 31.2% as compared to the year 2022. In the above mentioned 2023 report, financial fraud, sexual

exploitation and extortion are the majority of cases registered across the country.

With the emergence of cybercrime investigation, the nature of state power within the criminal justice system has simultaneously been altered. For instance, traditional investigative practices relied heavily on the collection of physical evidence, physical searches and seizure of documentary evidence. Whereas during cybercrime investigation, all the above-mentioned practices are being replaced by technologically intrusive forensic processes such as device imaging, remote extraction, metadata reconstruction, cloud extraction, behavioral mapping, and AI-assisted forensic analysis, which makes the investigation of cybercrimes more difficult than other criminal investigations.

Whenever any device is searched, and seizure during cybercrime investigation and digital forensic extraction is applied to it, it always raises the risk of privacy intrusion because such extraction often permits nearly total access to one's personal communications, financial records, location histories, and biometric identifiers. Therefore, it is not wrong to say that electronic devices are nothing but a mere extension of one's personhood in constitutional terms. Moreover, the Indian legal framework regulating cybercrime investigation fails to define the scope of digital search. For instance, it doesn't lay down any forensic extraction limits, protocols for cloning the device, requirement for any data minimization during digital forensic investigation.

It has been observed that Indian law enforcement authorities are relying heavily on institutional authorities like cyber cells, forensic labs, and electronic surveillance mechanisms during cybercrime investigation, which changes the nature of cybercrime investigation to a more techno-driven criminal investigative framework. As a result, it is the technological capabilities that play an important role in determining the directions of investigative authorities during cybercrime investigations.

Recently, India's procedural framework regulating cybercrime investigation has been updated with modern procedures in order to address the complexities of cybercrimes. For instance, Bharatiya Nagarik Suraksha Sanhita 2023 introduced updated search and seizure procedures; Bharatiya Sakshya Adhiniyam 2023 introduced modernize principle regarding the admissibility of electronic evidences, Digital Personal Data Protection Act, 2023 regulates the processing of digital personal data in order to protect the informational privacy of an individual. However, the above-mentioned laws are structurally fragmented as well as doesn't laid down any constitutional limits on forensic extraction and investigative data practices to be followed by investigative authorities. As a result, these structural asymmetries are easily demonstrated in institutional accountability, cyber forensic standards, evidentiary controls, as well as proportionality assessment during digital forensic investigations.

The main criticism of India's digital forensic framework is that it is inclined more toward evidence collection rather than protecting the fundamental rights of the suspect during digital forensic investigation. For instance, existing laws governing cybercrime investigation in India focus primarily on regulating the admissibility of electronic evidence instead of regulating the forensic process through which such evidence is extracted and preserved. Consequently, India still lacks a comprehensive legal framework regulating digital forensic extraction, data retention, chain of custody standards, forensic accountability, and forensic laboratories. Therefore, it can be said that technological upgrades in criminal investigations have expanded faster than constitutional and procedural safeguards.

Recognizing the right to privacy as an intrinsic part of Article 21 by the Indian judiciary in the Justice K.S. Puttaswamy case marked a constitutional watershed. However, the legal discourse in the matter of digital forensic investigation needs to be extended beyond the privacy-violation-centric approach to constitutional dignity under Article 21 because the continuous informational access, behavioral surveillance, and retrospective construction of personal life are activities that are often carried out by investigative authorities during the digital forensic extraction process. As a result, the relationship between the state and individual is structurally altered due to these activities.

Unrestricted extraction of personal information creates a risk of intrusive surveillance, informational outreach, evidentiary contamination, and disproportionate state intrusion. The above-mentioned concerns directly implicate informational privacy, dignity, procedural fairness under Article 21, and protection against self-incrimination under Article 20(3) of the Indian Constitution.

In the light of the above-mentioned backdrop, the present article attempts to critically evaluate whether India's existing legal framework effectively balances informational privacy and digital due process in cybercrime investigation. As well as the extent to which India's cyber forensic standards assure the authenticity and admissibility of electronic evidence without compromising privacy and dignity throughout the entire process.

## 2. CONSTITUTIONAL DIGNITY, INFORMATIONAL PRIVACY AND DIGITAL CRIMINAL INVESTIGATION

### *2.1. Evolution of Dignity Under Article 21*

Article 21 of the Indian Constitution guarantees the right to life and personal liberty to all, irrespective of the fact that they are citizens or non-citizens. Initially, the Indian Judiciary used to give a narrower interpretation of Article 21, that is it provides protection against arbitrary deprivation of life and personal liberty only. However, with the passage of time this interpretation gets broader by including in its ambit dignity, autonomy, personhood, and privacy of an individual. Such broader interpretation of Article 21 became possible only when the judiciary understands that the term "life" doesn't mean mere physical existence; rather, it should include within its ambit the right to live with dignity, mental autonomy, and informational freedom.

In order to have strong constitutional governance in a country, procedural fairness is considered one of its foundational pillars because it ensures that every state action that curtails the right to life and personal liberty of its citizens must not be arbitrary; rather, it must be just, fair, reasonable, non-arbitrary, and based on the principle of natural justice. Article 21 of the Indian Constitution, which guarantees life and personal liberty to all citizens and non-citizens, is not absolute; rather, restrictions can be imposed on the ground like "procedure established by law".

Initially, the Indian judiciary in the *A.K. Gopalan* case gave a narrow interpretation to the phrase "procedure established by law", but later on in the case of *Maneka Gandhi*the court gave an expansive application to the phrase "procedure established by law" and held that the procedure by which life and personal liberty can be curtailed must be fair, reasonable, just, non-arbitrary, and based on the principle of natural justice, thereby integrating procedural fairness within criminal investigation. It is because of the Maneka Gandhi judgment that the American Due process requirement was introduced in India, which was earlier rejected by Constituent Assembly debates due to its elastic and uncertain nature.

This transition reflects the evolution of the procedural fairness requirement in India from formal legality to substantive due process. "Procedure established by law" is the only test of formal legality. It means that there must be a law in existence. Whereas, in due process, the main emphasis is on qualitative assessment of law. It means the law in question must be fair, reasonable, and non-arbitrary.

Moreover, the introduction of "transformative constitutionalism" helps in further development of the idea of dignity under the Indian Constitution. Transformative constitutionalism means the Constitution should not be treated as a mere static document rather, it should be interpreted as a living instrument which possesses the power to protect the individual from arbitrary state actions. Therefore, it can be said that the role of dignity is not confined to mere moral values; rather, it also helps in imposing constitutional limitations upon coercive investigative power.

In the context of cybercrime investigation, maintaining the dignity of an individual becomes more important because digital forensics often permits nearly total access to the most intimate dimensions of one's personal life, such as communications, financial records, location histories, relationships, beliefs, and movement patterns. Consequently, the digital forensic investigation not only affects one's privacy but also constitutional personhood.

## *2.2 Privacy and Informational Autonomy*

The term "privacy" is not explicitly mentioned in the Indian Constitution; rather, it is derived through judicial interpretations. In the case of *Justice K.S. Puttaswamy**the*** right to privacy is recognized as an intrinsic part of the right to life and personal liberty by the Indian judiciary. The Court also observed that dignity, autonomy, and informational self-determination are the three core principles on which the right to privacy rests. It is because of the *Justice K.S. Puttaswamy judgment **that*** the constitutional foundation of informational privacy was firmly established.

The legitimate state aim, necessity, proportionality, legality requirement, and procedural due process are some of the doctrinal principles that are used to examine the constitutional validity of any State action violating the right to privacy. The entire goal of the proportionality test is to bring a balance between societal interest in carrying out criminal investigation and an individual's interest in protecting his fundamental right to privacy. When it comes to cybercrime investigations, satisfying the proportionality test becomes more crucial because nowadays devices contain complete information regarding one's personal life such as relationships, behavior, and ideology. So, whenever any device is seized, examined, and data is extracted from it, the risk of privacy intrusion always arises. Therefore, it can be said that satisfying the proportionality test in state actions ensures constitutional control over digital forensics investigations. However, the operationalization of this right within criminal procedure and policing practices remains underdeveloped.

The term "privacy" can be categorized into three parts, namely bodily, informational, and decisional privacy. Bodily privacy means protection will be granted against physical surveillance or unauthorized search and seizure. Informational privacy means that digital identity as well as the personal data of citizens will be protected. Decisional privacy means freedom will be ensured to citizens in matters of self-determination and personal choices. In this case, the court also observed that privacy granted under Article 21 of the Indian Constitution is not absolute; rather, reasonable restrictions can be imposed on it, but such restrictions should be within constitutional limits. Indian judiciary in this case also acknowledges the fact that the power of the state to carry out surveillance has expanded significantly in recent times due to the advancement of technology. These modern technologies help investigative authorities in the aggregation and profiling of personal information on an unprecedented scale. As a result, the risk of informational domination by state authorities always arises.

Similarly, in the case of ***Gobind*** and ***R. Rajagopal v. State of Tamil Nadu, the*** court recognizes informational privacy within the ambit of "liberty" guaranteed under the article 21 of the Indian constitution. Nowadays, every judicial interpretation centered around personhood and human dignity instead of property centric safeguards. This doctrinal shift in constitutional jurisprudence makes Indian laws at par with global human rights jurisprudence.

According to experts, "informational autonomy" means individual ability to control the collection, storage, dissemination and use of one's personal data. However, this "informational autonomy" principle is frequently violated during the digital forensic investigation because Indian laws don't lay down any forensic extraction limits, protocols for cloning the device, requirement for any data minimization. Moreover, the modern forensic investigative tools help our investigative authorities in recovering deleted files, locating browser histories, browsing behavior, tracing social media communications, extracting cloud data, decryption of encrypted files and much more. The above-mentioned extraction activities often exceed the investigative necessity test, thereby creating a disproportionate interference on one's informational privacy.

## *2.3. Data Collection, Retention and Profiling During Investigation*

The data collection, retention, forensic cloning of devices, and access to cloud storage are essential activities of cybercrime investigation. However, the issue of constitutional violation often arises when such data is stored/retained by investigative authorities for an indefinite period. Moreover, such concerns become more serious and need to be addressed in a timely manner, especially when the information stored has no relation to the offence committed and investigative profiling extends beyond the suspect.

Processing of data in India is now fully regulated with the enactment of the Digital Personal Data Protection Act, 2023 (hereinafter referred to as the Act of 2023). It is a significant step toward preventing misuse of data. However, Section 17(2)(a) of the Act of 2023 provides broad exemptions to our law enforcement authorities investigating criminal cases in the interest of sovereignty, security, and public order. These exemptions risk privacy protections guaranteed under Article 21 as well as weaken accountability mechanisms.

Recognizing privacy as a fundamental right is required not only for protecting individual rights but also for safeguarding democracy. For instance, freedom of thought, institutional accountability and dissent protection can be secured more effectively after recognizing right to privacy as an intrinsic part of Article 21. Moreover, the non-availability of comprehensive oversight mechanisms regulating cybercrime investigation, especially in matters of continuous behavioral monitoring and social-network mapping, might produce a deterrent impact on freedom of speech and expression and collective association guaranteed under the Indian Constitution.

It is the need of the hour that India's cyber law enforcement framework needs to be shifted from a security-centric model to a fundamental rights-compatible digital governance framework. To achieve this, substantive limits on the investigative powers of our law enforcement authorities in the form of judicial scrutiny, procedural accountability, as well as a clear statutory framework regulating cybercrime investigation must be imposed so that dignity in evidence collection, targeted surveillance, and investigative fairness can be ensured.

### *2.4. Principle of Self -Incrimination and Compelled Access*

Constitutional protection against self-incrimination and compelled access is guaranteed under Article 20(3) of the Indian Constitution. According to Article 20(3), no person can be compelled to reveal information based on his/her personal knowledge unless such person voluntary agree to it. Similarly, in the Selvi case, the Supreme Court held that narco analysis, brain mapping techniques, and polygraph tests, if conducted involuntary then such test, will be considered unconstitutional because it violates mental privacy and personal autonomy principles. In this case, the Court also observed that compulsion doesn't mean only physical compulsion; rather, it includes within it's ambit cognitive and testimonial compulsion as well.

In the present digital era, constitutional protection guaranteed under Article 20(3) as well as the Supreme Court judgment in the Selvi case becomes more crucial, especially when it comes to compelled decryption, forced disclosure of passwords, and biometric unlocking of devices during digital forensic investigation. Because digital devices nowadays contain complete information regarding one's personal life, such as relationships, behavior, and ideology. Therefore, compelled access to such devices may amount to compelled testimonial disclosure. Ultimately, it results in a violation of protection guaranteed under Article 20(3) of the Indian Constitution. Moreover, the absence of a comprehensive statutory framework specifically regulating cybercrime investigative practices and compelled digital access has substantially impacted dignity as well as failing to secure the informational privacy of a suspect during evidence collection and analysis.

## 3. DIGITAL FORENSIC INVESTIGATION PROCESS UNDER INDIAN CRIMINAL LAW

### *3.1. Nature and Scope of Digital Forensics*

The term "Digital Forensics" means a process which is scientific in nature and involves activities like identification, acquisition, preservation, analysis, and presentation of electronic evidence. All these activities are carried out so that the authenticity and admissibility of such electronic evidence can be established in judicial proceedings as well as during criminal investigations. Unlike conventional investigations, cybercrime investigations rely heavily on digital evidence. As a result, the nature of cybercrime investigation has transformed more into technological driven investigative process.

Initially, digital forensics involved limited evidentiary tools for evaluating digital evidence seized during cybercrime investigations. Currently, digital forensics has evolved and includes within it's ambit a wide variety of

forensic tools and technologies for surveillance and investigative reconstruction. Digital forensics can be further classified into the following categories: -

- Mobile device forensics- This forensic methodology often uses tools like Cellebrite and Oxygen to recover call records, chats, deleted messages, application data, geo-location histories, and encrypted information from suspected smartphone devices.
- Computer forensics- This forensic methodology is used by investigative authorities with the primary aim of extracting and recovering all the data from computers, hard disks, storage devices, and operating systems.
- Cloud-based forensics - This forensic methodology involves reconstructing metadata, processing cross-border data requests, and investigating and recovering stored digital data in cloud infrastructure.
- Metadata analysis forensics- This forensic methodology helps cybercrime investigative authorities to reconstruct the digital activities of suspects of crime through timestamps, device identifiers, geo-location markers, and browsing histories.
- Network forensics - This forensic methodology involves activities like analysis of internet traffic, reconstructing IP log, analysis of communication patterns, and data transmission records.
- Live forensics- This forensic methodology is frequently used by investigative authorities in cases of ransomware. This methodology involves analysis of volatile memory like RAM and network sessions.

## *3.2. Stage of the Digital Forensic Process*

### A. **Identification**

The first step in the entire digital forensic process begins with the identification of relevant digital devices, communication systems, storage media, and network infrastructures connected with the alleged offence. For instance, cybercrime investigators used to identify all the mobile phones, laptops, CCTV systems, servers, and cloud accounts, etc. In this process, all the devices identified for digital forensics must be proportionate and connected to the scope of investigation so that allegations of arbitrary exercise of power cannot be raised.

### B. **Seizure of Devices**

Seizure of digital devices connected with the alleged offence is a second step in an entire digital forensic process to be followed by investigative authorities. Under Indian criminal law, detailed search and seizure procedures for conventional criminal investigations have been mentioned. Consequently, seizure of electronic devices during cybercrime investigation is also regulated by this search and seizure procedure. India lacks a comprehensive search and seizure procedure designed especially for regulating seizure of digital devices during cybercrime investigation. Therefore, the risk of privacy intrusion is always there in case of unrestricted seizure of electronic devices because digital devices contain personal and unrelated information related to the suspect.

### C. **Preservation**

It is a third step in an entire digital forensic process. This step ensures that electronic devices seized during cybercrime investigation must not be altered from the time of seizure till production of such device before the court of law. In this step, the main challenge before investigative authorities is to secure such electronic devices against tampering, deletion of relevant information, remote access, and corruption of data stored in such devices. All this can be prevented only if the chain of custody is well documented by our investigative authorities from the time of seizure till production of such device before the court. Failure to maintain chain of custody by investigative authorities affects both reliability and admissibility of such devices in the court of law.

### D. **Forensic Imaging**

Forensic imaging of original devices with hash verification (MD5/SHA-256) in order to preserve the original devices without fabrication. This is a significant step to prove maintenance of the chain of custody during the investigative process.

E. **Extraction and Acquisition**

In this step, investigative authorities employ various digital forensic tools and technologies in order to extract and recover call records, chats, deleted messages, encrypted information, data stored in hard disks, storage devices etc. Contemporary forensic tools and technologies often give deep access into one's personal and behavioral information, extending beyond the alleged offence.

F. **Analysis and Recovery**

In this step, investigative authorities use various AI-assisted forensic analysis, behavioral mapping, meta reconstruction, automatic data filtering tools, and technologies to evaluate and establish digital timelines and criminal activities of a suspect before the court of law.

G. **Documentation and Reporting**

It is the last step to be followed by digital forensic investigator in the entire digital forensic process. In this step, the investigator prepares a forensic report containing the following details: -

- Extraction methods followed in order to derive relevant information connected with the alleged offence.
- Description regarding maintenance of chain of custody during this process.
- Description of evidence recovered.
- Forensic findings of digital forensic investigators.
- Integrated Verification procedures.

## *3.3. Investigative Powers under BNSS,2023*

India's existing legal framework has been updated recently to address the challenges posed by cybercrimes. Reforms have been made both in substantive laws as well as in procedural laws of India because the complexities of cybercrimes are not adequately addressed under the old legal framework; as a result, cyber offenders used to escape from the clutches of the law. Bharatiya Nagarik Suraksha Sanhita 2023 is introduced in place of the Code of Criminal Procedure, 1973.

Apart from the IT Act, the secondary legislation available in India that regulates investigative procedure in criminal cases is the Bharatiya Nagarik Suraksha Sanhita, 2023 (hereinafter referred to as BNSS,2023). One of the significant developments made under BNSS, 2023 is the introduction of electronic communication during the investigative process. For instance, BNSS,2023 allows electronic issuance and service of summons, notices, and other investigative communications during criminal investigation. This is a conceptual shift in investigative procedure because electronic modes of engagement is no longer mere auxiliary tools.

Similarly, BNSS, 2023 mandates the audio-video recording of search and seizure carried out during the investigation stage. However, it fails to lay down any separate chapter regulating digital privacy during examination of seized devices; no protection is provided in respect of non-relevant personal data stored in seized devices; there are no limits on forensic extraction, protocols for cloning the device, requirement for any data minimization during digital forensic investigation. As a result, it can be said that digital due process remains underdeveloped in the new legal regime.

Recently, the case of ***Virendra Khanna*** court addressed the issue of potential abuse at the time of seizure of electronic evidence as well as procedural lapses during cybercrime investigation. The court also emphasized the need for detailed guidelines regarding the search and seizure of electronic devices during cybercrime investigation. The court also highlighted that it is mandatory to ensure that the search should not exceed the scope of investigation. In this case, the court permits forensic imaging of the original device but cautioned that the examination must respect

necessity and relevance. The court also held that law enforcement agencies during investigation cannot engage in indiscriminate trawling of entire digital content. Similarly, in the case of **State of Goa (through the CID CS North Goa)**the court pointed out that the investigating officer who had seized CDs did not even know the meaning of the term harsh function and harsh value.

Moreover, section 176 clause (3) of BNSS, 2023 makes it mandatory for law enforcement authorities to take assistance of forensic experts during investigation of offence punishable with imprisonment of 7 years and more. However, such provisions cannot be effectively implemented unless our procedural laws include detailed search and seizure procedures to be followed during cybercrime investigation.

Failure to maintain authenticity and integrity of the chain of custody during investigation, such as improper documentation work, improper handling of fragile evidence during transit, lack of storage facilities etc, ultimately leads to inadmissibility of electronic evidence in the court of law. Therefore, in order to deal with cybercrime cases effectively, our law enforcement agencies require more advanced skills, efficient strategies, methods, technology, an updated legal framework, and proper training. Consequently, it can be said that BNSS has expanded the investigative powers of our authorities technologically, but it fails to create a comprehensive forensic governance structure regulating digital privacy during the search and seizure process. In the case of **Shibani Barik, the** court again stressed the need for proper training of cyber forensic investigators so that electronic evidence can be handled properly during investigation and transportation to forensic labs.

Unlike India, the United Kingdom has incorporated the proportionality principle in its legal framework in order to secure the privacy of its citizens during cybercrime investigation. For instance, the Police and Criminal Evidence Act 1984 (hereinafter referred as PACE,1984) laid down the comprehensive procedure regulating the search and seizure to be followed by investigative authorities during cybercrime investigation. Sections 19-20 of the PACE,1984 authorize law enforcement authorities to seize electronic records found during search and seizure; however, two restrictions in the form of relevance and necessity have been imposed on enforcement authorities seizing such electronic records. Similarly, section 22 deals with satisfaction of the proportionality principle before any data retention during criminal investigation. The entire digital search protocol has been mentioned under Code B of the PACE, 1984, which is not there in India. Moreover, Article 6 and 8 of the Human Rights Act 1998 operating in the UK include an exclusionary rule that allows the court to automatically exclude evidence obtained in violation of data protection norms.

### *3.4. Forensic Laboratories and Institutional Infrastructure*

The institutional infrastructure and forensic laboratories available in India for regulating digital forensic investigations are as follows:-

- Cyber crime cells created in every state, especially to handle the rising cyber crime cases in India.
- Central Forensic Science Laboratories
- State Forensic Science Laboratories
- The Indian Computer Emergency Response Team (CERT-In) is a national authority formed under the Ministry of Electronics and Information Technology (MeitY) for addressing cybersecurity. CERT-In deals with cybersecurity incidents related to the entire Indian cyberspace, including government networks, private sector systems, and individual users. CERT-In manages and coordinates responses to general cyber incidents, except those related to Critical Information Infrastructure (CII). The key functions of CERT-In mainly include issuing advisories, guidelines, and alerts regarding cyber threats and vulnerabilities.
- Cyber forensic experts - They play an important role by assisting the digital forensic investigators in data recovery, forensic imaging, malware analysis, and expert testimony before the court of law during the trial in order to establish the authenticity and reliability of electronic evidence.

However, India lacks a dedicated statutory framework regulating the functioning, standardization, and accreditation of Forensic laboratories and their methodology. As a result, there is a variation in working patterns as

well as the manner in which cyber forensic reports are prepared by these laboratories. Consequently, our investigative authorities find it difficult to establish the authenticity and reliability of electronic evidence before the court of law.

Unlike India, the United Kingdom has established a uniform legal and policy framework in the form of the Forensic Science Regulator Act 2021 that regulates the functioning, standardization, and accreditation of cyber forensic laboratories and forensic methodology. All this is done with the objective of reducing the variation of working patterns as well as the manner in which cyber forensic reports are prepared by these laboratories. Ultimately, it helps in proving the integrity of the chain of custody to the satisfaction of the court, thereby ensuring the admissibility of electronic evidence in court of law.

### *3.5 Privacy and Cyber Forensic Practices*

On the one hand, the usage of sophisticated cyber forensic methodologies and practices helps law enforcement agencies to achieve investigative efficiency during criminal investigation. But at the same time, following raises concerns also raised: -

1. Full device cloning and imaging might result in excess data collection. It means some personal information of the concerned person, which has no relation to the investigation, might be collected or stored; thereby, the informational privacy guaranteed under Article 21 of the Indian Constitution gets violated.

2. Examination of metadata can expose patterns of behavior of the concerned person which might be irrelevant to the investigation.

3. Article 20(3) of the Indian Constitution gives every accused the fundamental right not to disclose any self-incriminating statement. However, this fundamental right of an accused might be violated due to mandatory disclosure of encryption credentials.

4. Large-scale extraction of cloud-based stored information may fail to satisfy the proportionality test laid down in the Puttaswamy judgment if the warrant authorizing the same fails to prescribe in detail the scope and relevance of such bulk extraction.

5. Lack of mandatory prior judicial approval for carrying out digital search is another important concern during cybercrime investigation.

## 4. DATA PROTECTION, INVESTIGATIVE EXEMPTIONS AND DIGITAL DIGNITY UNDER DPDP ACT, 2023

The introduction of the Digital Personal Data Protection Act, 2023 (hereinafter referred to as the Act of 2023) is a significant step towards regulating the processing of digital personal data in India. Safeguarding the information privacy of an individual in India is one of the core objectives of the Act of 2023. The Act of 2023 is a primary legislation available in India that works toward establishing a horizontal data protection framework. As per Section 4 of the Act of 2023, personal data of any citizen can be collected and processed only for lawful purposes, and that too with the consent of data principals. Moreover, the Act of 2023 explicitly mentions the legitimate purposes for which data can be collected and processed by public and private entities. Informational autonomy of an individual is institutionalized by the Act of 2023 through sections 5 and 6. Section 5 of the Act of 2023 makes it mandatory for data fiduciaries (entities that collect data) to give notice to the data principal (whose data is being collected) regarding the purpose of collecting and processing personal data. Such notice must be given before obtaining the consent of the data principal. Similarly, section 6 of the Act of 2023 deals with obtaining consent of the data principal before data collection. However, the safeguards mentioned in sections 5 and 6 of the Act of 2023 are significantly diluted during criminal

investigation.

Section 7 of the Act of 2023 deals with “legitimate uses” of data collection. It explicitly mentions that data can be collected by law enforcement authorities even without the consent of the data principal for those functions of the

state which are authorized by law, such as performing sovereign functions of the state, complying with legal obligations, etc.Therefore, if any data is collected by our law enforcement authority for cybercrime investigation, then it will fall under the category laid down under section 7 of the said Act. One of the major criticisms of the Act of 2023 is that it fails to harmonize with criminal procedural laws, such as the BNSS and IT Act; rather, it recognizes lawful processing under Section 7 of the Act of 2023.

The data collection, retention, forensic cloning of devices, and access to cloud storage are essential activities of cybercrime investigation. However, when it comes to data retention, concerns regarding constitutional violations might be raised: -

- Storage of data for an indefinite period by investigative authorities,
- Information stored has no relation to the offence alleged to be committed and
- Investigative profiling by investigative authorities may extend beyond the suspect.

The Digital Personal Data Protection Act, 2023 is a significant step toward preventing misuse of data. However, Section 17(2)(a) of the Act of 2023 provides broad exemptions to our law enforcement authorities investigating criminal cases in the interest of sovereignty, security, and public order. These exemptions risk privacy protections guaranteed under Article 21 as well as signify wider executive discretion in matters of data protection. In India, no substantive limits on the investigative powers of our law enforcement authorities in the form of judicial scrutiny have been mentioned, whereas in the UK, a "Double lock" warrant in the form of approval from the executive and judiciary has been created under the Investigatory Powers Act, 2016.

The broad exemption created under the Act of 2023 does not mandate our law enforcement authorities to comply with necessity or the least intrusive means. Ultimately, the proportionality test laid down in the Puttaswamy case is diluted during cybercrime investigation. Section 18 of the DPDP Act has created the Data Protection Board of India. It is an independent adjudicatory body responsible for preventing data breaches, ensuring data privacy compliance by entities, and resolving disputes if any arise. However, the power of the Data Protection Board of India in the matters of data processing by law enforcement agencies remains ambiguous, thereby weakening the independent oversight mechanism in India. Detailed analysis of the DPDP Act, 2023 signifies that private entities are heavily regulated under the Act, whereas operations of State investigative agencies are exempted.

The Act of 2023 doesn't lay down any mandatory data minimization standards to be followed by our law enforcement authorities during search and seizure carried out in criminal investigations. It is often reported that during cybercrime investigations, our investigative agencies used to collect more personal data of a suspect than is required for investigation purposes. Consequently, such investigative practices violate the principle laid down under Section 8 of the Act of 2023. Moreover, the DPDP Act is silent with respect to the evidentiary value of the data obtained in violation of data protection norms, whereas in the UK, the exclusionary rule is followed; that is, UK courts can automatically exclude the evidence obtained in violation of data protection norms.

The enactment of the Digital Personal Data Protection Act, 2023 is a significant step by India legislature toward establishing baseline data protection standards. However, the broad exemptions carved out in favor of our law enforcement authorities create a parallel privacy regime which is protected from rigorous scrutiny by the data protection board created under the said Act. The Supreme Court, in the case of *Justice K.S. Puttaswamy,* laid down the legality, legitimate state aim, proportionality, and necessity tests to examine the constitutional validity of any State action violating the right to privacy of citizens. However, the 2023 Act fully satisfies the legality test but fails to adequately address the principles of necessity and least intrusive means in investigative procedures.

Unlike India, the United Kingdom Data Protection Act 2018 does not provide any broad exemptions to law enforcement authorities investigating criminal cases; rather, sections 31- 44 of the Data Protection Act 2018 regulate the processing of data by law enforcement authorities during digital investigation. Moreover, Article 5 of UK GDPR lays down mandatory data minimization and purpose limitation standards to be followed by law enforcement

authorities during search and seizure carried out in criminal investigation, thereby privacy obligations remain operative even during criminal investigation.

A detailed analysis of the Act of 2023 clearly shows that in India, privacy is conceptualized more as a regulatory compliance matter instead of a fundamental right-centric approach that imposes limitations on investigative power. Ultimately, privacy is placed below the sovereign functions of the state.

## 5. CONCLUSION AND SUGGESTIONS

The nature of criminal justice administration in India has transformed drastically with the rapid expansion of digital forensics in cybercrime investigation. In the present era, digital forensics tools and technologies have acquired a central role in the entire investigative process, especially in cybercrime cases, where finding the real culprit otherwise becomes very difficult for our law enforcement authorities if digital forensics technologies are not used by them. For instance, forensic imaging, mobile device forensics, cloud forensics, network forensics, metadata analysis, and behavioral reconstruction are some of the digital forensics technologies that are often employed by our investigative authorities during the examination of seized digital devices.

On the one hand, the usage of the above-mentioned technologies has expanded the extraction capabilities of our law enforcement agencies. But at the same time, these technologies also give unrestricted access to an individual's informational existence, such as personal communications, financial records, location histories, biometric identifiers, etc. As a result, the informational privacy, constitutional dignity, procedural fairness, and protection against self-incrimination guaranteed under the Indian Constitution are directly implicated by such unrestricted extraction of personal information by investigative authorities.

The present study makes it clear that though India’s existing legal framework has been updated to make it more technologically progressive, so that complexities posed by cybercrime cases can be addressed effectively. But it remains constitutionally fragmented, as it doesn't lay down any constitutional limits on forensic extraction, investigative data practices, chain of custody safeguard and, independent forensic oversight mechanisms, or forensic accountability to be followed by investigative authorities. In India, privacy has been recognized as a fundamental right by the Indian judiciary, but the absence of a comprehensive statutory framework specifically regulating cybercrime investigative practices has substantially impacted the dignity of an individual as well as failed to secure informational privacy during evidence collection and its analysis. India’s cybercrime investigation framework needs to be shifted from an executive-led model to a fundamental rights-compatible digital governance framework.

The following reforms need to be incorporated into India’s legal framework to secure informational privacy and constitutional dignity during digital forensic investigation: -

1. Mandatory compliance with the certification requirement laid down in section 63 of the BSA,2023

2. Electronic evidence should be sent to certified forensic laboratories only for examinations.

3. Mandatory documentation of every stage of the chain of custody.

4. Mandatory hash value verification.

5. Any electronic evidence obtained in violation of constitutional protection guaranteed under Article 21 and 20(3) should be excluded.

6. Similar to the UK Forensic Science Regulator Act, India too should establish a uniform legal and policy framework regulating the functioning, standardization, and accreditation of Forensic laboratories and their methodology. In the absence of such a statutory framework results in variation of working patterns as well as the manner in which cyber forensic reports are prepared by these laboratories. Ultimately, it affects the admissibility of electronic evidence in the court of law.

7. The proportionality clause must be explicitly mentioned in the broad exemptions created in favor of law enforcement authorities investigating criminal cases under Section 17 of the Act of 2023.

8. The jurisdiction of the Data Protection Board of India must be extended to data processing carried out by law enforcement authorities during cybercrime investigations, thereby strengthening the independent oversight mechanism in India.

**References**


1. Rahul Jain & Bhabani Sonowal, Cybercrime Unveiled: Technologies for Analyzing Legal Complexity (Springer International Publishing 2025) 266.
2. 'Crime patterns: On the National Crime Records Bureau's report for 2023' (The Hindu, 11 October 2025)<https://www.thehindu.com/opinion/editorial/crime-patterns-on-the-national-crime-records-bureaus-report-for-2023/article70148719.ece> accessed 21 May 2026.
3. National Crime Record Bureau, Report on Crime In India 2023 <https://www.ncrb.gov.in/crime-in-india.html> accessed 25 May 2026.
4. Kirankumar Akate Patil, 'Hurdles in Cyber Forensic Investigation in India' (2017) IOSR Journal of Computer Engineering.
5. Rahul Kailas Bharati, 'The New Criminal Law Paradigm in India and its Impact on Cybercrime Adjudication' (2026) SSRN < https://ssrn.com/abstract=5378219> accessed 18 May 2026.
6. Mr. Pratyaksh Joshi and Dr. Yogesh Wamankar, 'Algorithmic Policing And Due Process In Cybercrime Investigations: A Constitutional Analysis Under Articles 14, 19 And 21 of The Indian Constitution' (2025) 2 ShodhSamajik: Journal of Social Studies 153.
7. Dr. Anupam Kurlwal and Shreyansh, 'Evolution Of The Right To Privacy In India: Constitutional Perspective And Judicial Approach' (2024) 5(4) ShodhKosh: Journal of Visual and Performing Arts 1985.
8. The Constitution of India, art 21.
9. Ibid.
10. A.K. Gopalan v. State of Madras, AIR 1950 SC 27.
11. Maneka Gandhi v. Union of India, AIR 1978 SC 597.
12. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
13. Akanksha Singh, 'Right to Privacy: Exploring the Judicial Approach in this Digital Age' (2024) 8(1) Journal of Constitutional Law and Jurisprudence 91.
14. Davesh Grover, 'The Law Of Right To Privacy In India: Protecting Privacy In The Digital Era: Challenges' (2024) 5(1) ShodhKosh: Journal of Visual and Performing Arts 367.
15. Gobind v. State of Madhya Pradesh AIR 1975 SC 1378.
16. Kasim Patel, 'The Right To Privacy In Digital India: Analyzing The Personal Data Protection Framework' (2025) Record Of Law <https://recordoflaw.in/the-right-to-privacy-in-digital-india-analyzing-the-personal-data-protection-framework/ > accessed 22 May 2026.
17. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s 17(2)(a) .
18. The Constitution of India, art 20(3).
19. Selvi v. State of Karnataka (2010) 7 SCC 263.
20. Mehul Anand, 'Cybercrime And Cyber Laws In India' (2023) 5(2) Indian Journal of Law and Legal Research 1.
21. E. Casey, Digital Forensics and Investigation (Academic Press 2021).
22. H. Usha, Cyber Forensics: Digital Experience (5th edn, ICFAI University Press 2018).
23. Arpita Singh, 'A Framework for Crime Detection and Diminution in Digital Forensics' (2022) 13(2) International Journal of Advanced Computer Science and Application 332.
24. Rahul Kalias,'Digital Forensics and Electronic Evidence' <https://www.researchgate.net/publication/394304458_Digital_Forensics_and_Electronic_Evidence > accessed on 24 May 2026.
25. G. Usha, Cyber Forensics: Digital Experience (5th edn., ICFAI University Press 2018).
26. E. Casey, Digital Forensics and Investigation (Academic Press 2021).
27. A.K. Gopalan v. State of Madras, AIR 1950 SC 27.
28. Virendra Khanna v. State Of Karnataka & Ors. (2024) Air online 2021 Kar 525.
29. Vadita Agarwal & Tanishq Kabra, 'Self-Incrimination And Digital Evidence: Proposing A Framework Post Virendra Khanna' (2024) 17 NUJS L. Rev. 2.
30. State of Goa (through the CID CS North Goa) v. Tarunjit Tejpal (2021) SCC, Panaji Sessions & District Court.
31. Harsh Function is a function whose output values are all the same number of bits in length, especially one used to encrypt or compress data or to generate indices.

32. Harsh value means a function whose output values are all the same number of bits in length, especially one used to encrypt or compress data or to generate indices.
33. The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s 176(3).
34. Shibani Barik v. State of Odisha (2020) SCC Online 425.
35. Police and Criminal Evidence Act 1984, ss 19 and 20.
36. Human Rights Act 1998, arts 6 and 8.
37. Zareen Mirza, 'Cybercrime: A Systematic Study with UK, USA and India' 10 (2023) International Journal of Innovative Research in Engineering and Management 77.
38. Dr. Neeraj Malik, 'Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings as per Bhartiya Sakshya Adhiniyam, 2023' (2024) 11 Shodh Sagar Universal Research Reports 64.
39. The Digital Personal Data Protection Act, 2023 (Act 22 of 2000), s 4.
40. The Digital Personal Data Protection Act, 2023 (Act 22 of 2000), s 5.
41. S.Chandana, 'Critical Analysis of Cybersecurity Due Diligence And Its Impact On M&A Agreements Under The Digital Personal Data Protection Act, 2023 (DPDP Act)' (2025) 7 Indian Journal of Law and Legal Research 2023.
42. The Digital Personal Data Protection Act, 2023 (Act 22 of 2000), s 7.
43. Bharvi Shahi and Anand Raj Dev, 'Navigating India's Digital Personal Data Protection Act: Critical Implications and Emerging Challenges'(2025) 3 International Journal of Legal Studies and Social Science 415.
44. E. Casey, Digital Forensics and Investigation (Academic Press 2021).
45. Sonali Srivastav, 'India: Decrypting critical concepts under India's Digital Personal Data Protection Act, 2023 and comparison with GDPR and PIPL' (IJLT Blogs, 21 March 2024) < https://forum.nls.ac.in/ijlt-blog-post/india-decrypting-critical-concepts-under-indias-digital-personal-data-protection-act-2023-and-comparison-with-gdpr-and-pipl/? > accessed 27 May 2026.
46. Dr. Rahul Kailas Bharati, 'Cyber Law and Data Privacy in the 21st Century: Emerging Legal Issues and Challenges' (2025) 13 International Journal of Humanities Education 972.
47. Dr. Pradip Kumar Kashyap, 'Digital Personal Data Protection Act, 2023: A New Light into The Data Protection And Privacy Law In India' (2023) 2(2) ICREP Journal of Interdisciplinary Studies 3.
48. Sayed Aheed, 'Cyber Crimes, Law, and Cyber Forensics: Comparative Study of Indian, British, and American Contexts' (2024) 3 International Scientific Journal of Engineering and Management 2.
49. Anumodan Tiwari, 'Decoding the right to privacy in the Digital age: A critical analysis of Data protection laws in India under the DPDP ACT,2023' (2024) Lawful Legal <https://lawfullegal.in/decoding-the-right-to-privacy-in-the-digital-age-a-critical-analysis-of-data-protection-laws-in-india-under-the-dpdp-act-2023/? > accessed 26 May 2026.