Page: 1366-1399 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 2

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.205

BALANCING DATA PRIVACY AND DIGITAL FORENSIC INVESTIGATION IN INDIA: A CRITICAL ANALYSIS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND BHARATIYA SAKSHYA ADHINIYAM, 2023

Mayur Mahajan[1]

I. ABSTRACT

Today's digital landscape involves constant gathering, retention, and exchange of personal data via websites, apps, and online networks. The rapid rise in cybercrimes like hacking, online fraud, identity theft, and data breaches, driven by technological progress, has made digital forensic investigation a crucial component of the criminal justice system. This study investigates the interplay between data privacy and digital forensics in India, focusing specifically on the Digital Personal Data Protection Act and the Bharatiya Sakshya Adhiniyam of 2023. This research clarifies the definitions and boundaries of data privacy and digital forensics, while also examining the historical development of data protection and electronic evidence legislation in India. It also examines the constitutional dimensions of privacy, surveillance, and digital rights following the establishment of privacy as a fundamental right under Article 21. This study offers a critical examination of the 2023 DPDP Act and Bharatiya Sakshya Adhiniyam, focusing on their regulations concerning consent, data processing, electronic evidence, and investigative authority. The study further underscores the escalating tension between personal privacy and criminal probes. The study analyzes real-world obstacles in digital forensics, such as data encryption, cyber threats, technical skill gaps, and international cybercrimes. The research also examines key court rulings and contrasts India's regulatory structure with global data protection norms. The study asserts that while digital forensics are vital for national security and law enforcement, they require constitutional and legal protections to safeguard individual privacy and digital liberties. It further

[1] BBA LLB(H), 5th Semester, Student at Jaipur National University (India). Email: justmayurrrr.29@gmail.com

 (ISSN: 2583-7753)

indicates that India requires a digital investigation framework that is transparent, balanced, and focused on privacy. This study examines data privacy, digital forensics, and cybercrime under the 2023 DPDP Act and Bharatiya Sakshya Adhiniyam, focusing on electronic evidence, surveillance, and digital rights.

II. KEYWORDS

Data Privacy, Digital Forensics, DPDP Act 2023, Right to Privacy, Electronic Evidence.

III. INTRODUCTION

The swift progress of technology and the broad adoption of digital platforms have fundamentally reshaped how people communicate, store data, conduct business, and engage with society. In today's digital age, personal data has emerged as a highly valuable asset, sparking growing worries about privacy, security, and the potential misuse of digital information. The surge in cybercrimes, online fraud, identity theft, hacking, financial scams, and digital offenses has rendered digital forensic investigation essential for law enforcement and the criminal justice system. The dynamic between data privacy and digital investigation in India has grown more intricate and vital as technology advances.

Data privacy involves safeguarding individual information against unauthorized access, misuse, or disclosure. It guarantees that people retain authority over their personal information and online presence. Conversely, digital forensics encompasses the identification, gathering, preservation, analysis, and display of electronic data to support investigations and legal decisions. Although digital forensics are crucial for crime detection and prevention, their reliance on personal devices, communications, and sensitive data creates a direct tension between individual privacy rights and state investigative authority.

The Supreme Court's landmark decision in Justice K.S. Puttaswamy (Retd.) v. Union of India established that the Right to Privacy is a fundamental right protected under Article 21 as well as the broader framework of Part III of the Constitution, including Articles 14

and 19, thereby granting privacy full constitutional status in India.[2] This development intensified the urgency for a comprehensive legal framework to govern personal data protection. Thus, the passage of India's 2023 Digital Personal Data Protection Act represented a major advancement in governing how personal data is gathered, handled, and retained. Likewise, the 2023 Bharatiya Sakshya Adhiniyam established key rules governing the admissibility and evidentiary weight of electronic records in India's legal framework.

The growing reliance on digital evidence in criminal investigations has sparked numerous legal, ethical, and constitutional issues. Challenges such as state surveillance, unauthorized data access, insufficient consent, personal information misuse, and technological constraints persist in balancing individual privacy rights with effective law enforcement. Digital investigations are further complicated by practical challenges for investigative agencies, including encrypted devices, cross-border cybercrimes, data recovery problems, and rapidly evolving technologies. Concurrently, unchecked surveillance and boundless data gathering could endanger democratic principles and civil rights without adequate regulatory protection.

This study evaluates the interplay between data privacy and digital forensics in India, focusing on the legal and constitutional structures defined by the Digital Personal Data Protection Act and the Bharatiya Sakshya Adhiniyam of 2023. This research examines the development of data protection legislation, the probative weight of electronic evidence, court rulings on privacy and surveillance, and the practical difficulties encountered in digital inquiries. This study additionally examines global practices and underscores the ethical issues stemming from contemporary forensic methods and digital surveillance tools. The primary objective of this research is to evaluate whether the current legal framework in India effectively balances the interests of national security, criminal investigation, and individual privacy rights in the digital age. The paper seeks to provide

[2] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.

recommendations for developing a transparent, privacy-compliant, and technologically efficient forensic investigation system that protects both constitutional freedoms and the interests of justice.

A. Research Objectives

The present study seeks to examine the evolving relationship between data privacy and digital forensic investigation in India within the framework of the Digital Personal Data Protection Act, 2023 and the Bharatiya Sakshya Adhiniyam, 2023. The specific objectives of the study are:

1. To analyse the concepts, scope, and significance of data privacy and digital forensics in the digital age.
2. To examine the evolution of data protection and electronic evidence laws in India.
3. To evaluate the constitutional dimensions of privacy, surveillance, and digital rights under Article 21 of the Constitution of India.
4. To critically analyse the legal framework established under the Digital Personal Data Protection Act, 2023 and the Bharatiya Sakshya Adhiniyam, 2023.
5. To assess the evidentiary value of electronic records and the challenges associated with digital forensic investigations.
6. To examine judicial approaches towards privacy, surveillance, and electronic evidence.
7. To identify legal and practical challenges in balancing individual privacy rights with effective criminal investigation and national security requirements.

B. Research Questions

The study is guided by the following research questions:

1. What is the legal and constitutional relationship between data privacy and digital forensic investigation in India?

2. How have the Digital Personal Data Protection Act, 2023 and the Bharatiya Sakshya Adhiniyam, 2023 transformed the regulatory framework governing personal data and electronic evidence?
3. What constitutional safeguards govern state surveillance and access to personal data during criminal investigations?
4. What are the major legal, technological, and procedural challenges faced in digital forensic investigations?
5. Whether the present Indian legal framework adequately balances privacy rights, national security interests, and effective law enforcement in the digital environment?

C. Research Methodology

This study adopts a doctrinal, descriptive, and analytical research methodology. The research is primarily based on qualitative analysis of statutory provisions, judicial decisions, government reports, and scholarly literature relating to data privacy, digital forensics, surveillance, and electronic evidence.

Primary sources include the Constitution of India, the Digital Personal Data Protection Act, 2023, the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, relevant rules framed thereunder, and leading judicial pronouncements including Justice K.S. Puttaswamy v. Union of India, Anuradha Bhasin v. Union of India, Selvi v. State of Karnataka, and People's Union for Civil Liberties (PUCL) v. Union of India.

Secondary sources include books, journal articles, research papers, government publications, reports of the National Crime Records Bureau (NCRB), policy documents, and comparative international materials including the European Union General Data Protection Regulation (GDPR).

The study employs analytical and comparative methods to evaluate the adequacy of the existing legal framework and to assess the balance between privacy protection, digital investigation, and national security in contemporary India.

IV. CONCEPTUAL UNDERSTANDING AND SCOPE OF DATA PRIVACY AND DIGITAL FORENSICS

A. Meaning of Data Privacy

Data privacy refers to the protection and proper management of personal information in the digital environment. It ensures that individuals have control over how their personal data is collected, stored, processed, shared, and used by organizations, government authorities, and online platforms. Personal information may include names, contact details, financial records, biometric data, browsing history, location information, and other sensitive details that can identify a person.

In today's digital world, people continuously share information while using social media, online banking, e-commerce websites, healthcare applications, and communication platforms. As a result, concerns regarding misuse of personal data, identity theft, cyber fraud, and unauthorized access have increased significantly. Data privacy aims to protect individuals from such risks and maintain confidentiality, autonomy, and informational security.

The concept of data privacy is closely associated with the Right to Privacy, which was recognized by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India as a fundamental right protected under Article 21 and the broader guarantees contained in Part III of the Constitution, including Articles 14 and 19. This judgment emphasized that protection of personal data and informational privacy is essential for preserving human dignity and individual freedom in the digital age.

B. Meaning of Digital Forensics

Digital forensics is a branch of forensic science that deals with the identification, collection, preservation, examination, and presentation of electronic evidence for investigative and legal purposes. It involves recovering and analyzing data stored in digital devices such as computers, smartphones, servers, cloud storage systems, CCTV recordings, email accounts, and social media platforms.

The primary objective of digital forensics is to investigate cybercrimes and identify digital evidence that can be used in courts of law. Digital forensic experts follow scientifically accepted and legally recognized procedures to ensure that electronic evidence remains authentic, reliable, and admissible during judicial proceedings.

Digital forensics has become increasingly important due to the rapid growth of technology and digital communication. It plays a significant role in investigating crimes such as hacking, online fraud, identity theft, cyber terrorism, financial crimes, and data breaches. In addition to criminal investigations, digital forensics is also used in corporate investigations, cybersecurity management, and national security operations.

C. Scope and Importance in Modern Society

The scope of data privacy and digital forensics has expanded rapidly with technological advancement and increasing digitalization across different sectors of society. Governments, businesses, educational institutions, healthcare organizations, and financial institutions now heavily rely on digital systems and data-driven technologies for their daily operations. While this digital transformation has created opportunities for growth and innovation, it has also increased risks relating to personal data misuse and cybersecurity threats.

Data privacy has become essential for protecting individual dignity, personal autonomy, and informational security in a technology-driven society. Strong data protection mechanisms help build public trust in digital platforms and encourage the safe use of online services. In the absence of proper safeguards, individuals may become vulnerable to surveillance, profiling, identity theft, financial fraud, and misuse of sensitive information.

Similarly, digital forensics has become an indispensable part of modern criminal investigations and cybersecurity systems. Investigative agencies rely on electronic evidence such as emails, call records, CCTV footage, GPS data, and social media activity to detect crimes, identify offenders, and establish facts before courts. As cybercrimes and

digital offenses continue to rise globally, digital forensics have become crucial for maintaining law and order and ensuring national security.

D. Relationship Between Privacy and Investigation

The relationship between data privacy and digital forensic investigation is complex and often involves a conflict between individual rights and state interests. On one side, privacy laws seek to protect personal information from unauthorized access, misuse, and unnecessary surveillance. On the other side, digital investigations require access to electronic devices, communication records, and online data to investigate crimes and maintain public safety.

Investigating agencies frequently examine mobile phones, laptops, emails, social media accounts, and cloud storage systems to collect evidence relating to criminal activities. However, unrestricted or excessive access to such personal information may violate an individual's privacy and constitutional freedoms. The growing use of surveillance technologies, data interception systems, facial recognition tools, and mass monitoring mechanisms has further intensified concerns regarding misuse of power and invasion of privacy.

Therefore, it is necessary to maintain a balance between effective criminal investigation and protection of individual rights. While digital forensic investigation is important for ensuring law enforcement and national security, it must operate within constitutional and legal limits. Proper safeguards, judicial oversight, and accountability mechanisms are essential to prevent arbitrary surveillance and misuse of personal data in a democratic society.

V. EVOLUTION OF DATA PROTECTION AND ELECTRONIC EVIDENCE LAWS IN INDIA

A. Early Legal Framework

Before the introduction of specific cyber laws in India, legal issues relating to privacy, data protection, and electronic records were governed through traditional laws such as

the Indian Penal Code, 1860, the Indian Evidence Act, 1872, and constitutional principles. These laws were primarily designed for physical documents and conventional crimes and were not fully capable of addressing the challenges arising from digital technology and cyber-related offenses.

With the expansion of the internet and computer systems during the 1990s, India began witnessing new forms of crimes such as hacking, data theft, online fraud, and unauthorized access to computer systems. However, the absence of a dedicated legal framework created difficulties in investigating cybercrimes and recognizing electronic records as valid evidence before courts. The growing dependence on digital communication and electronic commerce further highlighted the need for specialized legislation to regulate digital transactions and cyber activities.

At the constitutional level, privacy was indirectly protected through Article 21 of the Constitution of India, which guarantees the Right to Life and Personal Liberty. Although the right to privacy was not expressly recognized in the early years, Indian courts gradually interpreted Article 21 broadly to include protection against arbitrary intrusion into personal life. This judicial development later became the foundation for modern data privacy laws in India.

B. Information Technology Act, 2000

The Information Technology Act, 2000 was the first comprehensive legislation enacted in India to regulate cyber activities and electronic communication.[3] The Act was introduced primarily to provide legal recognition to electronic records and digital signatures and to facilitate electronic commerce and e-governance. It was enacted based on the UNCITRAL Model Law on Electronic Commerce to align India's legal system with international digital standards.

The Information Technology Act, 2000 played a significant role in establishing the legal foundation for cyber law in India. It recognized electronic records as legally valid

[3] Information Technology Act 2000.

documents and enabled electronic contracts and digital transactions. The Act also introduced provisions relating to cyber offenses such as hacking, identity theft, data theft, cyber terrorism, and unauthorized access to computer systems.

Over time, the Act was amended to strengthen data protection and cybersecurity measures. The Information Technology (Amendment) Act, 2008 introduced Section 43A, which imposed liability on body corporates for negligence in protecting sensitive personal data. It also introduced Section 72A, which penalized disclosure of personal information obtained through lawful contracts without consent. Additionally, the government framed the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 to regulate the handling of sensitive personal data by corporate entities.

Despite these developments, the Information Technology Act, 2000 was criticized for lacking a comprehensive framework for personal data protection and privacy rights. The provisions relating to data protection were limited in scope and did not adequately address issues such as consent, data processing, accountability, and rights of individuals over their personal information.

C. Development of Electronic Evidence Laws

The increasing use of digital devices and online communication significantly transformed the nature of evidence in criminal and civil proceedings. Emails, electronic records, CCTV footage, mobile phone data, social media content, and digital documents gradually became important sources of evidence before courts. This created a need to legally recognize and regulate electronic evidence within the Indian judicial system.

The Indian Evidence Act, 1872 was amended through the Information Technology Act, 2000 to incorporate provisions relating to electronic records. Sections 65A and 65B were introduced to establish special rules regarding the admissibility of electronic evidence.[4]

[4] Indian Evidence Act 1872, ss 65A–65B.

Section 65B became particularly important because it prescribed the conditions under which electronic records could be admitted as evidence before courts.

The judiciary has played a crucial role in shaping the law relating to electronic evidence in India. Several landmark decisions have clarified the interpretation of Section 65B of the Indian Evidence Act, 1872 and the conditions governing admissibility of electronic records. In State (NCT of Delhi) v. Navjot Sandhu,[5] the Supreme Court permitted admission of certain electronic evidence through alternative modes of proof even in the absence of a certificate under Section 65B. However, this position was expressly overruled in Anvar P.V. v. P.K. Basheer,[6] where the Court held that compliance with Section 65B is a mandatory requirement for admissibility of electronic records when such records are produced in the form of secondary evidence.

The legal position was subsequently reaffirmed and comprehensively clarified in Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal,[7] wherein the Supreme Court reiterated the mandatory nature of Section 65B certification and explained the limited circumstances in which the certificate requirement may be relaxed. These decisions collectively established procedural safeguards intended to preserve the authenticity, reliability, and evidentiary integrity of electronic records in judicial proceedings.

With the introduction of the Bharatiya Sakshya Adhiniyam, 2023, India further modernized its evidentiary framework by giving greater recognition to electronic and digital records. The new legislation reflects the changing nature of technology-driven investigations and acknowledges the growing importance of digital evidence in the criminal justice system.

D. Need for Modern Data Protection Legislation

The rapid growth of digital technology, social media platforms, e-commerce, cloud computing, artificial intelligence, and online services resulted in massive collection and

[5] S*tate (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 600.
[6] *Anvar PV v PK Basheer* (2014) 10 SCC 473.
[7] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

processing of personal data by both private companies and government authorities. This increased concerns regarding surveillance, misuse of personal information, data breaches, identity theft, and lack of accountability in handling personal data.

India lacked a dedicated and comprehensive data protection law for many years. The limited provisions under the Information Technology Act, 2000 were insufficient to address modern privacy challenges arising from large-scale digital data processing. Furthermore, the recognition of the Right to Privacy in Justice K.S. Puttaswamy (Retd.) v. Union of India as a fundamental right flowing from Article 21 and the broader protections contained in Part III of the Constitution created a constitutional obligation upon the State to establish a robust legal framework for protecting personal data.

The need for modern legislation became more urgent due to increasing global focus on data protection laws such as the European Union's General Data Protection Regulation (GDPR).[8] India required a structured framework that could regulate consent, data collection, processing, storage, transfer, and accountability while balancing innovation, economic growth, and individual privacy rights.

As a result, the Digital Personal Data Protection Act, 2023 was enacted to provide a comprehensive legal framework governing personal data protection in India.[9] The Act aims to regulate the processing of digital personal data, establish rights and obligations for individuals and data fiduciaries, and create mechanisms for accountability and grievance redressal. It represents a major step toward strengthening privacy protection and ensuring responsible use of personal data in India's rapidly evolving digital ecosystem.

VI. CONSTITUTIONAL PERSPECTIVE ON PRIVACY, SURVEILLANCE, AND DIGITAL RIGHTS

[8] Regulation (EU) 2016/679 (General Data Protection Regulation).
[9] Digital Personal Data Protection Act 2023.

The Indian Constitution ensures fundamental rights that safeguard the dignity, liberty, and personal freedom of every individual. Even though the Constitution does not explicitly state a Right to Privacy, the judiciary has read this right into Article 21's guarantee of the Right to Life and Personal Liberty, thereby establishing privacy as an essential constitutional right. As people constantly disclose personal details via online services, social networks, digital payments, and communication tools in today's digital era, safeguarding privacy has grown ever more critical.

The 2017 landmark ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India represented a historic milestone in Indian constitutional jurisprudence, as the Supreme Court unanimously affirmed that the Right to Privacy is a fundamental right protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a component of the freedoms guaranteed under Part III of the Constitution, including Articles 14 and 19. The Court noted that privacy is intrinsically connected to human dignity, autonomy, control over personal information, and individual liberty.

Acknowledging privacy as a constitutional right profoundly reshaped India's legal landscape concerning data protection and digital governance. As technology advances rapidly, worries about unauthorized data access, surveillance, profiling, identity theft, and information misuse have grown significantly. Concurrently, the State is turning more heavily to surveillance tools to uphold national security, ensure public order, prevent crime, and conduct criminal investigations.

Contemporary surveillance techniques encompass phone tapping, internet monitoring, CCTV, facial recognition, biometric systems, and the interception of electronic communications. While these actions might advance valid government goals, overly broad or capricious monitoring can infringe upon constitutional liberties and personal privacy.

In the Puttaswamy ruling, the Supreme Court laid down key principles regulating state intrusion into privacy. The Court ruled that any limitation on privacy must meet the criteria of legality, necessity, proportionality, and legitimate state interest. Consequently,

surveillance operations must be grounded in legal authorization, directed toward a legitimate purpose, and conducted without being disproportionate or arbitrary. Consequently, judicial review and procedural protections are essential to curb the potential abuse of surveillance authorities and shield the public from capricious government conduct.

The rise of digital rights has broadened the constitutional debate surrounding privacy and technology. Digital rights encompass informational privacy, free expression online, internet access, data security, and safeguards against illegal digital intrusions. In Anuradha Bhasin v. Union of India, the Supreme Court affirmed that internet access is integral to exercising the freedom of speech and expression guaranteed under Article 19(1)(a).[10] This ruling underscored the increasing constitutional importance of digital liberties in contemporary society.

India has also enacted the Digital Personal Data Protection Act, 2023, a legislative measure designed to govern the collection, processing, and safeguarding of personal data to address privacy concerns. Nevertheless, harmonizing national security, technological progress, efficient law enforcement, and personal privacy rights remain one of the most formidable constitutional hurdles in the rapidly changing digital age.

A. Key Points

1. The Right to Privacy is protected under Article 21 of the Constitution of India.
2. *Justice K.S. Puttaswamy v. Union of India (2017)* recognized privacy as a Fundamental Right.
3. Privacy includes informational privacy, bodily integrity, and personal autonomy.
4. Digital technologies have increased concerns regarding misuse of personal data and unauthorized surveillance.

[10] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.

5. State surveillance is conducted for national security, crime prevention, and public order.
6. Modern surveillance methods include phone tapping, internet monitoring, CCTV systems, and facial recognition technologies.
7. Excessive surveillance may violate constitutional rights and individual freedoms.
8. The Supreme Court established the principles of legality, necessity, proportionality, and legitimate state interest for restricting privacy rights.
9. Judicial oversight and procedural safeguards are essential to prevent misuse of surveillance powers.
10. Digital rights include privacy, freedom of expression, internet access, and protection of personal data.
11. *Anuradha Bhasin v. Union of India* highlighted the constitutional importance of internet access and digital freedom.
12. The Digital Personal Data Protection Act, 2023 was introduced to strengthen data protection and digital privacy in India.
13. Balancing national security and individual privacy remains a major constitutional challenge in the digital age.

VII. LEGAL FRAMEWORK OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The rapid growth of digital technology has significantly increased the collection and use of personal data in India. Online transactions, social media platforms, digital payments, biometric systems, and e-governance services continuously process personal information. While digitalization has improved connectivity and governance, it has also raised concerns regarding privacy, surveillance, data breaches, and misuse of personal information. To address these challenges, India enacted the Digital Personal Data

Protection Act, 2023 (DPDP Act, 2023), which provides a legal framework for protection and regulation of digital personal data.

The constitutional basis of the Act lies in the landmark judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), where the Supreme Court recognized the Right to Privacy as a fundamental right protected under Article 21 and the broader framework of Part III of the Constitution, including Articles 14 and 19. The judgment emphasized the importance of informational privacy and the need for legal safeguards against arbitrary data collection and surveillance.

A. Objectives of the Act

The major objectives of the DPDP Act 2023 are:

1. Protection of personal data and informational privacy.
2. Regulation of collection, storage, and processing of digital personal data.
3. Establishment of accountability for organizations handling personal information.
4. Prevention of data breaches and misuse of personal data.
5. Balancing privacy rights with State interests such as national security and public order.

B. Important Features of the Act

The Act recognizes individuals as "Data Principals" and entities processing data as "Data Fiduciaries." Personal data can generally be processed only after obtaining free, informed, and specific consent from the individual. The Act also grants important rights to individuals, including:

1. Right to access personal data.
2. Right to correction and erasure data.
3. Right to grievance redressal.
4. Right to withdraw consent.

The Act further imposes obligations upon Data Fiduciaries to maintain security safeguards, prevent data breaches, and erase data after the purpose of processing is fulfilled. Certain organizations categorized as "Significant Data Fiduciaries" may also be required to appoint Data Protection Officers and conduct audits.

VIII. STATE EXEMPTIONS, PRIVACY CONCERNS, AND THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025

One of the most debated aspects of the DPDP Act is the broad exemption granted to the State in matters relating to national security, sovereignty, public order, and prevention of offences. Critics argue that excessive government powers and limited judicial oversight may weaken privacy protections and increase risks of digital surveillance. The legal framework was substantially strengthened through the notification of the Digital Personal Data Protection Rules, 2025, which operationalise the Act and establish detailed obligations for Data Fiduciaries and Significant Data Fiduciaries.

The Rules introduce a phased implementation framework consisting of Stage I (November 2025), which brought into force foundational provisions and established the Data Protection Board of India**;** Stage II (November 2026), which activates the registration and regulation of Consent Managers; and Stage III (May 2027), which brings into effect core compliance obligations relating to notices, consent management, security safeguards, data breach reporting, grievance redressal, and obligations of Significant Data Fiduciaries.

The Rules also prescribe operational requirements concerning breach notifications, maintenance of security safeguards, audit mechanisms, and accountability measures. These developments are particularly significant for digital forensic investigations because organizations handling personal data are now required to maintain stronger documentation, security controls, and incident-response mechanisms, thereby improving the integrity and traceability of electronic evidence. At the same time, concerns remain regarding the scope of governmental exemptions under the Act and Rules, particularly

in relation to surveillance, access to personal data during investigations, and the adequacy of independent oversight mechanisms. Consequently, the DPDP Rules, 2025 play a crucial role in shaping the balance between privacy protection and legitimate investigative interests in India's evolving digital governance framework.[11]

Data Analysis: - India currently has:

1. Category	Approximate Data
2. Internet Users	850+ Million
3. Smartphone Users	700+ Million
4. Social Media Users	450+ Million

According to NCRB reports, cybercrime cases increased from approximately 27,000 cases in 2018 to more than 65,000 cases in 2022.[12] This rapid rise in cyber offenses highlights the necessity of a strong data protection framework in India.

IX. NATURE, PROCESS, AND EVIDENTIARY VALUE OF DIGITAL FORENSIC INVESTIGATION

Digital forensics has become a vital element of today's criminal justice framework. As communication, finance, and personal interactions shift toward digital platforms, crimes increasingly leave behind electronic traces. Today, mobile phones, emails, CCTV footage, cloud storage, GPS records, and social media messages serve as vital evidence in criminal investigations.

[11] Digital Personal Data Protection Rules 2025, notified by the Ministry of Electronics and Information Technology on 13 November 2025; Government of India, Establishment of the Data Protection Board of India (14 November 2025).
[12] National Crime Records Bureau, *Crime in India*.

Digital forensics is the scientific methodology used to identify, gather, preserve, analyze, and present electronic evidence in legal proceedings. Its main goal is to guarantee that digital evidence stays authentic, reliable, and admissible in court. Unlike conventional evidence, electronic records are exceptionally susceptible to modification and removal, rendering procedural protections and forensic precision critically vital.

Typically, a digital forensic investigation proceeds through the stages of seizing electronic devices, extracting data, preserving evidence, conducting a forensic examination, and drafting expert reports. Investigative bodies often depend on digital evidence when probing cybercrime, financial fraud, terrorism, identity theft, online harassment, and organized crime. As reliance on digital proof expands, the importance of forensic specialists within the criminal justice framework has grown substantially.

The Bharatiya Sakshya Adhiniyam, 2023 confers legal status on electronic records as documentary proof and bolsters the evidentiary weight of digital materials in court proceedings. Digital evidence, including emails, WhatsApp messages, call logs, CCTV recordings, and online transaction histories, is now routinely submitted in court proceedings. Nevertheless, admissibility hinges on authenticity, integrity, and adherence to procedural safeguards governing electronic evidence.

NCRB data shows that cybercrime cases in India rose from approximately 27,000 in 2018 to over 65,000 in 2022, underscoring the expanding role of digital investigations. With over 850 million internet users and widespread smartphone adoption, India's rapidly growing digital landscape has heightened the importance of forensic technologies in criminal investigations.

Although critical, digital forensic investigations confront multiple hurdles such as encrypted devices, potential data tampering, insufficient technical expertise, limited infrastructure, and the complexities of cross-border cyber cases. Such obstacles frequently complicate the preservation of the chain of custody and the assurance of electronic evidence reliability.

Consequently, digital forensic inquiry has become essential for effective law enforcement in the modern digital age. Yet, the growing reliance on electronic monitoring and digital proof also brings forth significant issues regarding privacy, procedural equity, and constitutional protections within the criminal justice framework.

X. PRIVACY RIGHTS AND CRIMINAL INVESTIGATION: EMERGING CONFLICTS

The proliferation of digital technology has fundamentally reshaped the dynamic between privacy and criminal investigation. Contemporary investigative bodies are increasingly leveraging mobile devices, surveillance video, digital correspondence, social platforms, biometric records, location tracking, and cloud repositories to uncover criminal activity and pinpoint suspects. Although digital surveillance and electronic evidence bolster law enforcement capabilities, they concurrently raise significant apprehensions about informational privacy, state overreach, and the potential misuse of personal data. Consequently, a constitutional clash arises between two rival interests: safeguarding individual privacy and the state's authority to investigate.

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) firmly established the constitutional basis for privacy in India, wherein the Supreme Court affirmed that the Right to Privacy is a fundamental right protected under Article 21 and the broader guarantees contained in Part III of the Constitution, including Articles 14 and 19. The Court determined that informational privacy constitutes a fundamental component of dignity, liberty, and personal autonomy. Simultaneously, the ruling established that privacy is not an absolute right and can be limited by state measures that are lawful, necessary, and proportionate. This rule holds especially critical weight in criminal probes that rely on digital monitoring and electronic data.

The matter of surveillance was previously considered in People's Union for Civil Liberties (PUCL) v. Union of India (1997), wherein the Supreme Court reviewed the constitutionality of telephone tapping pursuant to the Telegraph Act. The Court ruled

that intercepting communications without authorization breaches the Right to Privacy and underscores the need for procedural protections, legal authority, and executive accountability in surveillance operations. The ruling determined that state surveillance must not be exercised at will and must instead adhere to constitutional constraints.

In Anuradha Bhasin v. Union of India (2020),[13] the Supreme Court affirmed that the exercise of freedom of speech and expression and the freedom to carry on trade or business through the internet are constitutionally protected under Articles 19(1)(a) and 19(1)(g) of the Constitution. The Court held that restrictions on internet access must satisfy the requirements of legality, necessity, and proportionality. This ruling underscored the increasing constitutional significance of digital rights and internet-based freedoms in contemporary governance and criminal justice frameworks.

The clash between privacy and investigation has grown sharper as surveillance tools including facial recognition, metadata analysis, internet interception, spyware, and AI-based monitoring become more prevalent. Agencies conducting investigations frequently defend such actions by citing national security, public order, and crime prevention as their rationale. However, surveillance that is too extensive and lacks sufficient judicial review threatens to turn lawful investigations into perpetual state monitoring.

In Selvi v. State of Karnataka (2010), the Supreme Court also underscored the need to shield individuals from non-consensual incursions into their mental privacy while reviewing narco-analysis, polygraph tests, and brain mapping procedures. The Court ruled that investigative methods lacking consent infringe upon personal liberty and the safeguard against self-incrimination guaranteed by Article 20(3). The ruling underscored that investigative expediency must not supersede constitutional protections and human dignity.

[13] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.

The growing reliance on digital evidence has further sharpened this constitutional controversy. NCRB data indicates that cybercrime incidents in India rose from roughly 27,000 in 2018 to over 65,000 by 2022. Modern investigative bodies now routinely incorporate WhatsApp messages, bank statements, GPS tracking, surveillance video, social media interactions, and digital communication records into their case files. As India's digital ecosystem expands, the volume of personal data accessible to investigative authorities has increased significantly.

The Digital Personal Data Protection Act, 2023 attempts to regulate data processing and strengthen privacy protection. However, the legislation also grants broad exemptions to the State in matters relating to sovereignty, national security, and prevention of offenses. Critics argue that excessive executive discretion and limited independent oversight may weaken constitutional privacy protections recognized in *Puttaswamy*.

Thus, the conflict between privacy rights and criminal investigation reflects a broader constitutional challenge in the digital age. A democratic State must possess sufficient authority to investigate crimes and maintain security, but such authority cannot operate without constitutional discipline. The principles of legality, necessity, proportionality, and procedural fairness remain essential to ensure that technological advancement does not erode individual liberty and democratic accountability.

XI. CONSENT, DATA PROCESSING, AND STATE SURVEILLANCE IN DIGITAL INVESTIGATIONS

The proliferation of digital technologies has markedly amplified the gathering, retention, and analysis of personal information within India. Mobile apps, social networks, digital banking, biometric repositories, and e-government tools constantly produce vast amounts of personal data. Although this digital infrastructure has enhanced governance and communication, it has also heightened worries about privacy, surveillance, and the potential misuse of personal data. Consequently, the constitutional issue involves

striking a balance between conducting effective digital investigations and safeguarding informational privacy and individual autonomy.

Under the Digital Personal Data Protection Act, 2023, consent serves as the foundational requirement for legally processing personal information. The Act stipulates that consent must be given freely, with full knowledge, specifically, without conditions, and clearly. People must be told what personal information is being gathered, why it is being processed, and how it might be used or shared. The legislation also empowers individuals to revoke consent and request corrections or deletions of their personal information. These measures bolster informational self-determination and embody the constitutional acknowledgment of privacy in the digital era.

Yet, the matter grows more intricate when viewed within the frameworks of criminal probes and government monitoring. Law enforcement agencies often depend on tools such as phone tapping, internet monitoring, CCTV, facial recognition, GPS tracking, and access to electronic records to prevent and investigate crimes. Although these actions can advance valid state goals like national security and public order, overly broad or capricious monitoring risks violating constitutional guarantees and democratic liberties.

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) firmly established the constitutional basis for privacy by recognizing the Right to Privacy as a fundamental right protected under Article 21 and the wider framework of Part III of the Constitution, including Articles 14 and 19. The Court ruled that informational privacy is a fundamental component of dignity and personal liberty, while also stressing that any limitation on privacy must adhere to the principles of legality, necessity, proportionality, and procedural safeguards. In People's Union for Civil Liberties (PUCL) v. Union of India (1997), the Supreme Court ruled that telephone tapping and communication interception represent grave intrusions into privacy, thereby mandating procedural safeguards and executive accountability.

The courts have also underscored the need to shield individuals from overly intrusive investigative measures. In Selvi v. State of Karnataka (2010), the Supreme Court ruled

that involuntary narco-analysis, polygraph tests, and brain mapping infringe upon personal liberty and the right against self-incrimination guaranteed by Article 20(3). Similarly, in Anuradha Bhasin v. Union of India,[14] the Court affirmed that the exercise of freedom of speech and expression and the freedom to carry on trade or business through the internet are protected under Articles 19(1)(a) and 19(1)(g) of the Constitution. The Court observed that restrictions on internet services must be lawful, proportionate, and subject to periodic review, thereby reinforcing constitutional safeguards applicable to digital communication and online activities.

The increasing significance of digital surveillance can be grasped by examining India's swiftly growing digital landscape.

Table 1: Digital Expansion in India

Category	**Approximate Data**
Internet Users	850+ Million
Smartphone Users	700+ Million
Social Media Users	450+ Million
Monthly UPI Transactions	Billions

The increase in digital users has also resulted in significant growth in cyber-related offenses and dependence on electronic evidence during investigations.

[14] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.

Table 2: Growth of Cybercrime Cases in India

Year	Registered Cybercrime Cases
2018	Approx. 27,000
2020	Approx. 50,000
2022	More than 65,000

The increasing dependence on digital evidence has expanded the scope of state access to personal information. At the same time, concerns continue regarding broad exemptions granted to government agencies under the DPDP Act, 2023 in matters relating to national security, sovereignty, and prevention of offenses. Critics argue that excessive executive discretion and lack of independent oversight may weaken constitutional privacy protections and create risks of mass surveillance.

Thus, the issue of consent, data processing, and state surveillance reflects a larger constitutional debate concerning the limits of state power in the digital age. While effective criminal investigation remains essential for maintaining law and order, constitutional democracy equally requires protection of privacy, dignity, and informational autonomy. Technological advancement cannot become a justification for unrestricted surveillance or erosion of individual liberty within a democratic society.

XII. ADMISSIBILITY, EVIDENTIARY STANDARDS, AND CHALLENGES OF ELECTRONIC EVIDENCE UNDER INDIAN LAW

A. Legal Framework Governing Electronic Evidence

The admissibility of electronic evidence in India was initially governed by Sections 65A and 65B of the Indian Evidence Act, 1872, introduced through the Information Technology Act, 2000. These provisions established special procedures relating to

admissibility of electronic records in judicial proceedings. Subsequently, the Bharatiya Sakshya Adhiniyam, 2023 modernized the evidentiary framework by granting wider recognition to digital and electronic evidence. Under Indian law, electronic records are treated as documentary evidence, provided they satisfy procedural requirements relating to authenticity, integrity, and reliability.

B. Types of Electronic Evidence

Electronic evidence includes emails, WhatsApp chats, CCTV footage, mobile phone records, social media communication, GPS data, cloud-stored information, online banking records, electronic contracts, and digital photographs. The rapid growth of digital communication and internet usage has significantly expanded the role of electronic evidence in criminal investigations, cybercrime cases, financial frauds, and commercial disputes.

1. **Evidentiary Standards for Electronic Records:** The admissibility of electronic evidence depends upon compliance with procedural safeguards established under law. Electronic records must remain authentic, reliable, and free from tampering or manipulation. Investigating agencies are required to maintain proper chain of custody during collection, preservation, and forensic examination of digital evidence. Courts also emphasize certification requirements to ensure reliability and evidentiary value of electronic records during judicial proceedings.
    - **Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023:** The Bharatiya Sakshya Adhiniyam, 2023 has significantly modernised India's legal framework governing electronic evidence. While the Indian Evidence Act, 1872 regulated electronic records through Sections 65A and 65B,[15] the new legislation introduces a dedicated framework under Sections 61, 62, and 63.[16] Section 61 recognises electronic and digital records as

[15] Indian Evidence Act 1872, ss 65A–65B.
[16] Bharatiya Sakshya Adhiniyam 2023, ss 61–63.

documentary evidence and places them on a similar evidentiary footing as traditional documents. Section 62 expands the scope of admissible electronic records by expressly acknowledging information generated, stored, transmitted, or received in digital form. Most importantly, Section 63 establishes the conditions governing admissibility of electronic records and substantially replaces the former Section 65B framework. Under Section 63, electronic records must satisfy requirements relating to authenticity, reliability, and integrity. A significant development under Section 63(4) is the requirement that the certificate accompanying an electronic record be authenticated not only by the person occupying a responsible official position in relation to the operation of the relevant device or management of the activities concerned, but also by an expert. This requirement strengthens the evidentiary reliability of digital evidence by introducing an additional layer of technical verification. From a digital forensic perspective, the expert-certification requirement enhances confidence in the authenticity of electronic records and reduces the risk of manipulation, tampering, or fabrication. However, it may also increase compliance burdens for investigating agencies, forensic laboratories, and law-enforcement authorities, particularly in cases involving large volumes of digital evidence. The revised framework reflects the growing importance of scientific validation in electronic evidence while seeking to balance evidentiary reliability with procedural efficiency in criminal investigations.

2. **Growth of Electronic Evidence in India:** The increasing use of smartphones, internet services, digital payments, and social media platforms has significantly increased dependence upon electronic evidence during investigations. Rising cybercrime cases, online frauds, identity theft, and digital financial offenses have made electronic records central to modern criminal justice administration. Investigating agencies frequently rely upon

WhatsApp chats, CCTV recordings, GPS records, online transaction logs, and social media activity while conducting criminal investigations.

3. **Practical and Technical Challenges:** Despite its growing importance, electronic evidence presents several practical and technical difficulties. Digital records are highly vulnerable to tampering, deletion, and unauthorized modification. Investigating agencies often face challenges in recovering encrypted or deleted data and maintaining proper chain of custody during forensic examinations. Lack of technical expertise, inadequate forensic infrastructure, rapidly evolving cyber technologies, and cross-border cyber investigations further complicate the process of digital evidence collection and admissibility.
4. **Constitutional and Privacy Concerns:** The growing dependence on electronic evidence also raises concerns regarding privacy and state surveillance. Access to personal devices, communication records, biometric information, and online activity may infringe upon informational privacy protected under Article 21 of the Constitution. Therefore, while electronic evidence strengthens criminal investigations, investigative procedures must operate within constitutional safeguards relating to legality, proportionality, procedural fairness, and protection of individual liberty.

XIII. JUDICIAL TRENDS, NATIONAL SECURITY, ETHICAL CONCERNS, AND FUTURE PROSPECTS OF DIGITAL PRIVACY AND FORENSICS IN INDIA

With the rapid growth of technology and internet usage, digital privacy and forensic investigation have become important parts of the Indian legal system. Today, crimes are no longer limited to physical spaces. Cybercrimes such as online fraud, hacking, identity theft, data breaches, financial scams, and cyberstalking are increasing rapidly. As a result, investigating agencies and courts now heavily depend upon electronic evidence such as

WhatsApp chats, emails, CCTV footage, mobile phone records, GPS data, and social media activity during investigations and trials.

Indian courts have played an important role in protecting privacy while allowing effective criminal investigation. In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Supreme Court recognized the Right to Privacy as a fundamental right protected under Article 21 and the broader guarantees contained in Part III of the Constitution, including Articles 14 and 19. The Court held that personal information and digital data are closely connected with human dignity and liberty. Similarly, in *People's Union for Civil Liberties (PUCL) v. Union of India (1997)*, the Supreme Court stated that phone tapping and surveillance must follow legal procedures and proper safeguards. These judgments show that investigative powers cannot be used without constitutional limitations.

At the international level, countries have also introduced strong privacy protection laws. The European Union's General Data Protection Regulation (GDPR) is considered one of the strongest data protection laws in the world.[17] It focuses on informed consent, data protection, transparency, accountability, and strict penalties for misuse of personal information. India has attempted to strengthen its digital privacy framework through the Digital Personal Data Protection Act, 2023 and the Bharatiya Sakshya Adhiniyam, 2023. However, concerns still remain regarding government surveillance powers and lack of independent oversight mechanisms.

National security is one of the major reasons behind digital surveillance and forensic investigations. Government agencies increasingly use facial recognition systems, biometric databases, CCTV networks, internet monitoring, and electronic interception to investigate terrorism, cybercrime, financial fraud, and organized criminal activities. While these mechanisms help maintain public safety and law enforcement, excessive

[17] Regulation (EU) 2016/679 (General Data Protection Regulation).

surveillance may violate privacy rights and democratic freedoms if not properly regulated.

Ethical concerns have also become important in digital investigations. Unauthorized access to personal devices, misuse of private information, data leaks, and continuous digital monitoring may affect individual dignity and informational autonomy. There are also concerns regarding manipulation of electronic evidence, lack of transparency in surveillance systems, and misuse of artificial intelligence technologies during investigations. Therefore, proper legal safeguards and accountability mechanisms are necessary to prevent abuse of digital powers.

India's digital growth further highlights the importance of privacy protection and digital forensic systems. India currently has more than 850 million internet users and over 700 million smartphone users. At the same time, cybercrime cases have increased significantly from nearly 27,000 cases in 2018 to more than 65,000 cases in 2022 according to NCRB reports. This increasing digital dependence has made electronic evidence and forensic investigation essential for modern criminal justice administration.

The future of digital privacy and forensic investigation in India depends upon maintaining a balance between technological advancement, national security, and constitutional rights. Stronger judicial oversight improved forensic infrastructure, technical training, transparency in surveillance practices, and effective implementation of privacy laws are necessary to protect both security and individual liberty.

In conclusion, digital forensic investigation and electronic evidence have become indispensable in the modern legal system. However, increasing use of surveillance technologies also creates serious privacy and ethical concerns. Therefore, India must continue developing a balanced legal framework that protects national security while ensuring privacy, dignity, and constitutional freedoms in the digital age.

XIV. SUGGESTIONS AND RECOMMENDATIONS

1. Clear statutory safeguards should be introduced to regulate access to personal data during digital investigations.
2. Judicial authorization should be strengthened for intrusive surveillance measures involving interception, device searches, and data extraction.
3. Independent oversight mechanisms should be established to review surveillance activities undertaken on grounds of national security and public order.
4. Digital forensic laboratories should be upgraded through improved infrastructure, technical resources, and specialised training.
5. Uniform national protocols should be developed for preservation, collection, and examination of electronic evidence.
6. Greater transparency and accountability should be incorporated into government data-processing and surveillance practices.
7. Stronger safeguards should be adopted to protect encrypted communications and sensitive personal data while permitting lawful investigations under constitutional standards.
8. International cooperation mechanisms should be strengthened to address cross-border cybercrime and digital evidence collection.
9. Public awareness programmes should be conducted to promote digital literacy, cybersecurity awareness, and privacy protection.
10. Future amendments to the DPDP Act 2023 should ensure a more balanced approach between privacy rights and legitimate state interests.

XV. CONCLUSION

The rapid expansion of digital technology has fundamentally transformed both personal privacy and criminal investigation in India. The enactment of the Digital Personal Data

Protection Act 2023 and the Bharatiya Sakshya Adhiniyam, 2023 represents a significant legislative effort to address the challenges arising from extensive data processing, cybercrime, and growing reliance on electronic evidence. At the constitutional level, the recognition of privacy as a Fundamental Right in Justice K.S. Puttaswamy v. Union of India has established important safeguards against arbitrary state intrusion into personal information and digital communications.

At the same time, digital forensic investigation has become indispensable for combating cybercrime, financial fraud, terrorism, and other technology-driven offences. The increasing dependence upon electronic evidence requires investigative agencies to maintain high standards of authenticity, reliability, and procedural fairness. However, the expanding use of surveillance technologies and broad governmental access to digital data continue to raise concerns regarding proportionality, accountability, and protection of individual liberties.

The study concludes that neither privacy rights nor investigative powers can be treated as absolute. A balanced legal framework must ensure that effective law enforcement operates within constitutional limits governed by legality, necessity, proportionality, and judicial oversight. As India's digital ecosystem continues to expand, future reforms should focus on strengthening privacy protections, improving forensic capabilities, enhancing transparency in surveillance practices, and ensuring that technological advancement remains consistent with constitutional values, democratic governance, and the rule of law.

XVI. REFERENCES

A. Cases

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
3. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
4. Selvi v. State of Karnataka, (2010) 7 SCC 263.

5. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
6. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.

B. Statutes

1. Constitution of India, 1950.
2. Information Technology Act, 2000.
3. Information Technology (Amendment) Act, 2008.
4. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
5. Digital Personal Data Protection Act, 2023.
6. Bharatiya Sakshya Adhiniyam, 2023.
7. Indian Evidence Act, 1872.
8. Indian Penal Code, 1860.

C. Government Reports and Official Sources

1. National Crime Records Bureau (NCRB), Crime in India Reports (2018–2022).
2. Ministry of Electronics and Information Technology (MeitY), Government of India, Digital Personal Data Protection Act, 2023 – Official Publications.
3. Parliamentary Debates and Legislative Materials relating to the Digital Personal Data Protection Act, 2023.

D. International Sources

1. European Union, General Data Protection Regulation (Regulation (EU) 2016/679).
2. UNCITRAL Model Law on Electronic Commerce, 1996.

E. Books and Journal Articles

1. Avtar Singh, Cyber Law and Information Technology (latest ed.).

2. Justice Yatindra Singh, Cyber Laws.

3. Relevant peer-reviewed articles on data privacy, digital forensics, electronic evidence, and surveillance law cited in the manuscript.