

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

The Right to Privacy and Cybercrime in India: A Critical Analysis of Legal Protection and Emerging Challenges

S. SRINIVASAN* AND DR. K. MURUGADOSS**

ABSTRACT

The dramatic growth of digital technologies has not only redefined the nature of violations of privacy but also strengthened the link between informational autonomy, cybersecurity and criminal liability. Cybercrimes increasingly involve identity theft, unauthorised access to information, cyberstalking, the non-consensual dissemination of images, data breaches, digital impersonation and technologically facilitated intrusion. This poses a fundamental legal question: does India's constitutional and legal architecture sufficiently protect individuals from violations of digital privacy and, at the same time, allow the proportionate investigation of cybercrime? In upholding the right to privacy in Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court established a constitutional foundation for the protection of dignity, autonomy and informational privacy. Constitutional recognition must, however, be translated into effective legal remedies, institutional accountability and safeguards. The paper critically analyses the constitutional dimensions of the right to privacy under Articles 14, 19 and 21 of the Constitution of India, the scope of the provisions of the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, intermediary responsibilities and the emerging framework of the Digital Personal Data Protection Act, 2023, and draws on decisions relating to interception and surveillance, the dissemination of personal information, internet restrictions and spyware allegations. Using a doctrinal and analytical approach based on legislation and judicial pronouncements, the paper argues that the main impediment in India is not the absence of legal protection but the multiplicity of remedies, the difficulty of proving culpability in cybercrime, and the 'silos' of privacy, public security and surveillance. It suggests a proportionate, rights-based framework that addresses these concerns through balanced investigation procedures, safeguards for digital evidence, accountable data-governance practices, independent oversight mechanisms and remedies for victims.

Keywords: *Right to Privacy, Cybercrime, Informational Privacy, Cybersecurity, Data Protection, Digital Surveillance*

* Author is a Research Scholar at Bharath Institute of Law, Bharath Institute of Higher Education and Research (BIHER), Chennai, Tamil Nadu, India.

** Author is a Dean of Law at Bharath Institute of Law, Bharath Institute of Higher Education and Research (BIHER), Chennai, Tamil Nadu, India.

I. INTRODUCTION

Digital tools are now woven into the fabric of banking, health, learning, work, governance and communication. People routinely share personal details through digital payments, social media, apps, biometric identity systems and online services. While this advances convenience and access, it also provides both the means and the motive for unauthorised access, identity theft, intrusive surveillance and the misuse of personal data. Cybercrime represents a distinctive threat to privacy, since information stored on computers can be duplicated, combined, transmitted and stored on a scale unprecedented in human history. A single hack can reveal the contents of private conversations, bank accounts, intimate photographs and information about one's friends and family. Data retrieved during one crime can later be used for identity theft, extortion and abuse, long after the attack itself has stopped, because such data persists on the web.

Privacy must therefore be understood not merely as secrecy, or as security from physical intrusion, but as personal autonomy, informational control, dignity and freedom from unwarranted interference with one's private life. Even without hacking, the collection, storage and processing of personal data can endanger private life. Unjustified intrusions through excessive surveillance, disproportionate profiling and unwarranted disclosure of information may also threaten individual autonomy. With the nine-judge Bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,¹ the constitutional position in India was decisively altered. Privacy was no longer a grey area, or a subordinate interest liable to be compromised by the State. It was a fundamental right, protected by the guarantees of Part III and by the right to life and personal liberty in Article 21.² In practice, however, enforcing privacy rights is more difficult. Cybercrime is often committed by anonymous actors, from outside the country, using encrypted communication, and the evidence is frequently held by private companies.

The same technology that is used for good can be used for malicious purposes, which makes it hard to determine who is responsible from the technology alone. The legal regime in India consists of constitutional law, the Information Technology Act, 2000 (IT Act),³ criminal law, intermediary regulations and the Digital Personal Data Protection Act, 2023 (DPDP Act).⁴ Each addresses a particular dimension of the problem, but their interface raises issues of legal certainty, remedies, coordination between bodies of law and between institutions, and the balance between security and rights. Effective privacy protection requires not just the

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

² INDIA CONST. art. 21.

³ Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

⁴ Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

recognition of privacy as a constitutional right and the enactment of a privacy law, but a cohesive approach that identifies criminal conduct and distinguishes it from lawful technological activity, places adequate duties on institutions, assists digital investigations and offers effective recourse to victims.

A. Research problem

The key problem to be researched is the disconnect between the constitutional acknowledgement of privacy and the practical effectiveness of legal measures against cybercrime. Although Indian law criminalises many acts in relation to computers and acknowledges privacy as a fundamental right, breaches of digital privacy tend to cross several legal domains and present complex evidentiary issues. This can leave victims unsure about where to turn for recourse, and law enforcement unsure about which legal standards to apply.

B. Research questions

This article addresses four questions:

1. How effective is the Indian constitutional framework in safeguarding individuals against infringement of their privacy through cybercrime?
2. To what extent do the IT Act, the Bharatiya Nyaya Sanhita, 2023 (BNS) and the developing DPDP framework deal with violations of digital privacy?
3. What principles have Indian courts used to strike a balance between privacy and surveillance, security and free speech?
4. What legal and institutional reforms are needed to make accountability a reality and to secure remedies proportionate to the harm suffered by victims of cybercrime?

C. Study objectives

The specific aims are to:

1. explore the constitutional underpinnings of privacy in India;
2. critically analyse the statutory provisions applicable to privacy-related cybercrimes;
3. review judicial pronouncements on surveillance and informational autonomy; and
4. suggest reforms, within the constitutional paradigm, for effective cybercrime investigation and enforcement and for institutional accountability.

D. Research methodology

This article uses a doctrinal and analytical approach; it discusses constitutional provisions, statutes, delegated legislation, case law and official notifications. Comparative principles are

applied where they help to explain regulatory choices, but the article focuses primarily on Indian law. The approach is qualitative, and the article does not claim to identify empirical patterns in the incidence or prosecution of cybercrime. Laws are read according to their text, as interpreted by the courts, and with regard to their dates of commencement.

II. CONCEPTUAL FOUNDATIONS OF THE RIGHT TO PRIVACY

A. Privacy as a multidimensional right

Privacy consists of bodily, spatial, decisional and informational interests. Bodily privacy concerns intrusion upon the physical person; spatial privacy concerns intrusion into a person's physical space; decisional privacy concerns intimate personal choices; and informational privacy concerns the collection, use, storage and dissemination of a person's information.⁵ These aspects converge in cybercrime. Spyware may compromise the informational privacy of a mobile phone user's intimate communications, photographs, location history and close relationships. The dissemination of private photographs may breach informational privacy as well as dignity and autonomy.⁶ Identity theft may leave a person vulnerable to financial abuse. A further challenge of the digital environment is aggregation. Apparently 'harmless' data such as location records, purchase history, search terms and social networks can be combined to reveal very private details about a person's movements, associations and activities. A purely individual conception of privacy may therefore be too narrow, and data about groups and aggregated data need protection too.⁷

B. Informational privacy and personal autonomy

Informational privacy concerns the circumstances in which personal information is collected, used, stored and disclosed. It does not, as such, confer a right to full access to and control over every fact relating to oneself. The right to informational privacy is significant because of its connection to autonomy. Data principals may be deprived of the ability to make meaningful choices in their digital lives if their data is taken without transparency, exploited for other purposes and disseminated indiscriminately. The outcomes can include discrimination, exploitation, reputational damage and criminal abuse. The law must therefore protect against the exposure of data through unlawful access to a database, and equally against the irresponsible use of data that was accessed lawfully. A database may, for example, contain data that an

⁵ Puttaswamy, *supra* note 1, at 263–64.

⁶ *Id.* at 263–64.

⁷ ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD/LEGAL/0188 (as amended July 11, 2013), <https://legalinstruments.oecd.org/public/doc/114/body-text.en.html>.

employee accessed lawfully, yet the employee's disclosure of that information breaches the law.⁸

C. Privacy and cybersecurity

Privacy and cybersecurity are interrelated but not interchangeable, and their legal meanings differ. Cybersecurity aims to protect computer systems and information against unauthorised access, alteration, disruption or deletion. Privacy concerns whether the collection, use and disclosure of information is appropriate and justified. Processing that is technically secure can still violate privacy if too much information is gathered or if monitoring is unwarranted. Conversely, a security breach can violate privacy even when the data was gathered lawfully. The concepts are distinct because technical security is no substitute for legal rules on processing. System security, law enforcement, data governance and constitutional protections must therefore be combined. Focusing on the technology while neglecting how data is processed would overlook the question whether there is a valid legal ground for the processing.

III. PRIVACY AS A CONSTITUTIONAL RIGHT IN INDIA

A. Article 21 and the development of privacy case law

Article 21 provides that 'No person shall be deprived of his life or personal liberty except according to procedure established by law'. The judiciary has interpreted it expansively to include not only life in the physical sense but also dignity and autonomy. In *Kharak Singh v. State of Uttar Pradesh*, the Supreme Court examined police surveillance and its impact on personal liberty. The later decision in *Gobind v. State of Madhya Pradesh* recognised the constitutional importance of privacy and discussed the scope of permissible restrictions. These judgments contributed to the incremental constitutional development that ultimately led to the recognition of privacy as a fundamental right.⁹

In *Puttaswamy*, the Court rejected the argument that the Constitution's silence on 'privacy' meant that privacy lacked constitutional protection. The Court held that privacy is part of life and personal liberty under Article 21 and is also linked with the Part III freedoms.¹⁰ This is especially relevant to the digital setting, in which privacy is not confined to the physical environment. The reasoning underlying the decision leaves room to examine the gathering of information, the monitoring of communications, identity systems and technological practices

⁸ *Id.* ¶ 10 (Use Limitation Principle).

⁹ *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295; *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.

¹⁰ *Puttaswamy*, *supra* note 1.

that affect individual freedom and autonomy.¹¹ It also makes clear that privacy cannot be overridden merely for administrative convenience.

B. Legality, necessity and proportionality

Recognition of the right to privacy does not mean that every interference is an infringement. The State may interfere for several reasons, such as criminal investigation or national security, but the interference must satisfy the relevant test. It must be authorised by law, and the law must be adequate; the fact that surveillance would be advantageous cannot alone justify an intrusion upon privacy.¹² Legitimate aim means that the State must have a rational and constitutionally acceptable reason for interfering with privacy. Necessity means that the measure must be reasonably necessary and that no less invasive option is available. Proportionality means that the measure must be proportionate to the aim.

Protections against unexplained use are equally vital. A digital investigation might uncover information about people who are not the subject of the investigation: family, friends, colleagues, journalists and advisers. Collecting an entire device or account could reveal far more information than is needed to investigate a particular offence. A privacy-sensitive analysis will therefore have to determine the legal basis, purpose, extent, time frame and safeguards associated with the operation.¹³ The analysis must be fact-specific: the constitutional right does not mean that every targeted investigative measure is invalid in advance, but neither does an investigative measure justify itself.

C. Articles 14 and 19

Article 14 is relevant to oppressive or discriminatory laws, and where surveillance or enforcement is arbitrary or discriminatory.¹⁴ Information technology may enable or exacerbate discrimination if the processing of personal data is directed disproportionately against particular groups. Articles 19(1)(a) and 19(1)(c) protect expression and association.¹⁵ Intrusive surveillance can chill lawful speech, political engagement, journalism and association regardless of whether the person monitored is ever prosecuted, so the constitutional analysis must examine its impact on democratic engagement more broadly. In *Anuradha Bhasin v. Union of India*, the Court dealt with restrictions on internet services. It held that restrictions must conform to legal requirements and that orders suspending services must be published. Although

¹¹ *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.

¹² *Puttaswamy*, *supra* note 1.

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

¹⁴ INDIA CONST. art. 14.

¹⁵ INDIA CONST. art. 19(1)(a), (c).

the case was not an ordinary cybercrime case, it shows that measures of digital governance must be tested against the requirements of legality and proportionality.

D. Positive obligations and private interference

Constitutional privacy applies principally to State action. Not every dispute between private persons amounts to a direct violation of a fundamental right by a private person. It is nonetheless important for the State to ensure an effective legal framework where the violation is committed by private persons or corporations.¹⁶ The disregard of privacy manifested in the unauthorised publication of private images, persistent cyberstalking and identity theft shows why substantive access to legal relief against private interference remains vital.¹⁷ A constitutional guarantee of privacy would be hollow if the law acknowledged the right in theory but not in practice. The State therefore has a duty to restrain private abuse while ensuring that enforcement powers remain proportionate.

IV. STATUTORY FRAMEWORK OF PRIVACY-RELATED CYBERCRIME

A. The Information Technology Act, 2000

The IT Act is the principal statute governing computer-related offences in India. Its relevant sections deal with hacking, identity theft, online impersonation, certain privacy violations and breaches of confidentiality. Section 43 provides for compensation for certain unauthorised acts in relation to computer systems and networks, including access, the copying or downloading of information, the introduction of contaminants, damage to computer resources and the disruption of access.¹⁸ This section may be relevant where an intrusion affects personal information or computer resources.

Section 66 makes the acts described in Section 43 offences when they are done dishonestly or fraudulently. The mental element is important: proving unauthorised access does not necessarily prove every element of the offence.

Section 66C deals with identity theft through the fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature. It is relevant to credential theft, account compromise and digital impersonation.

¹⁶ Digital Personal Data Protection Act, *supra* note 4, §§ 4, 8.

¹⁷ Information Technology Act, *supra* note 3, §§ 66C, 66E, 67, 67A.

¹⁸ *Id.* §§ 43, 66.

Section 66D punishes cheating by personation by means of a communication device or computer resource.¹⁹ It may be invoked where offenders pose as other persons or bodies to obtain money or confidential information.

Section 66E deals with intentionally or knowingly capturing, publishing or transmitting an image of a private area of a person²⁰ without his or her consent, in circumstances violating privacy. The offence is punishable with imprisonment for a term which may extend to three years, or with a fine which may extend to two lakh rupees, or with both. The provision addresses a specific problem that has arisen on the internet, particularly image-based abuse.

Section 72 deals with breaches of confidentiality and privacy by a person who, having secured access to material by virtue of powers conferred under the Act or the rules made under it, discloses that material to any other person without the consent of the person concerned. Section 72A punishes the disclosure, in breach of a lawful contract, of personal information by a person (including an intermediary) who obtained access to that information while providing services, in the circumstances specified.²¹

These provisions create distinct offences and ought not to be confused:

1. Sections 43 and 66 relate to particular unauthorised acts involving computers;
2. Sections 66C and 66D relate to identity-theft offences;
3. Section 66E relates to a specific type of privacy invasion involving private images; and
4. Sections 72 and 72A relate to specific disclosures.

The IT Act does not create a general offence of breach of online privacy. The applicable section depends on the facts: the type of information involved, the conduct complained of and the requirements of the section.

B. Section 43A and the data-protection transition

Section 43A of the IT Act provides for compensation where a body corporate that possesses, deals with or handles sensitive personal data or information is negligent in implementing and maintaining reasonable security practices and procedures, and thereby causes wrongful loss or wrongful gain. It is read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.²² Although the DPDP Act,

¹⁹ *Id.* §§ 66C–66D.

²⁰ *Id.* § 66E.

²¹ *Id.* §§ 72, 72A.

²² Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Apr. 11, 2011).

2023 applies to the wider category of digital personal data, it is being brought into force in phases. By Notification No. G.S.R. 843(E) of 13 November 2025, the Central Government appointed different dates for different provisions. Section 44(2) of the DPDP Act, which omits Section 43A of the IT Act, comes into force eighteen months after the publication of that notification, that is, on 13 May 2027; as of October 2026, therefore, Section 43A remains in force.²³ This intermediate position is significant from both a research and a legal perspective. It would not be correct to say that Section 43A has already been repealed, or that all substantive duties under the DPDP Act are immediately binding and enforceable. The precise legal position must be ascertained with regard to the specific commencement date of each provision.

C. The Digital Personal Data Protection Act, 2023

The DPDP Act provides a legal framework for the processing of digital personal data and defines concepts such as Data Principal, Data Fiduciary and the Data Protection Board of India.²⁴ Its framework includes notice, consent, certain legitimate uses, the duties of Data Fiduciaries, security safeguards, personal-data breaches, the rights of individuals and penalties. The Act is important because it recognises that protecting privacy requires organisations that process digital personal data to bear responsibilities for its protection, and not merely that hackers face criminal penalties. It can strengthen governance by defining responsibilities for data processing and creating an accountability framework.

Under G.S.R. 843(E), the institutional and administrative provisions of the Act, including Sections 2, 18 to 26 and 38 to 43, came into force on 13 November 2025. Section 6(9) and Section 27(1)(d), which concern Consent Managers, come into force one year after publication, on 13 November 2026, while the principal substantive provisions, including Sections 3 to 17, come into force eighteen months after publication, on 13 May 2027. The Digital Personal Data Protection Rules, 2025 likewise provide for phased commencement.²⁵ As of October 2026, the institutional structure has been set up, but the critical substantive obligations and individual rights have not yet come into effect. The Act must therefore be viewed as a system of law that is still being brought into force, rather than one whose substantive parts already govern conduct. Nor is the DPDP Act a substantive criminal code.²⁶ It regulates processing and allocates

²³ MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, Notification No. G.S.R. 843(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025), <https://egazette.gov.in/WriteReadData/2025/267647.pdf> [hereinafter Commencement Notification]; Digital Personal Data Protection Act, *supra* note 4, § 44(2).

²⁴ Digital Personal Data Protection Act, *supra* note 4, §§ 2, 4–10, 11–17.

²⁵ Commencement Notification, *supra* note 23; Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i), r. 1(2)–(4) (Nov. 13, 2025), <https://egazette.gov.in/WriteReadData/2025/267650.pdf>.

²⁶ Digital Personal Data Protection Act, *supra* note 4, § 33 & sched. (monetary penalties imposed by the Data Protection Board).

responsibilities with respect to digital personal data; offences such as identity theft, unauthorised access and intimate-image abuse continue to be prosecuted under the IT Act and other criminal laws.

D. The Bharatiya Nyaya Sanhita, 2023

The BNS also contains offences that may be attracted by privacy-related cybercrime. Section 78 criminalises stalking, including, in the specified context, monitoring a woman's use of the internet, email or any other form of electronic communication.²⁷ Its application depends on the elements of the offence and the facts of the case. Section 318, which deals with cheating, may be pertinent to online fraud,²⁸ where its conditions are met. Depending on the nature of the conduct, the offences of criminal intimidation, sexual offences, forgery or another relevant offence might also be made out.²⁹

The IT Act and the BNS may thus address separate aspects of the same act. An incident involving digital impersonation together with ongoing harassment and threats may call for reliance on both computer-related offences and general criminal-law provisions, but the statutory elements of each offence must be established separately. For conduct that took place before the BNS came into force on 1 July 2024, the applicable criminal law must be ascertained under the relevant temporal rules.

E. Intermediary responsibility

Offending material may be distributed through online platforms: intimate material may be published, or content created to impersonate or harass. Section 79 of the IT Act protects intermediaries that qualify for safe harbour. Rules 3 and 4 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Rules) impose due-diligence and grievance-redressal obligations.³⁰ Intermediary protection is not complete immunity, but the mere presence of illegal content on a platform does not mean that the operator has committed a criminal offence. The operator's obligations, the statutory conditions, its knowledge and its response to a lawfully issued notice must all be taken into account.

In *Shreya Singhal v. Union of India*, the Supreme Court read down the knowledge requirement in Section 79(3)(b),³¹ holding that an intermediary's obligation to act on 'actual knowledge' of

²⁷ Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023), § 78.

²⁸ *Id.* § 318.

²⁹ *Id.* §§ 63–73 (sexual offences), 336 (forgery), 351 (criminal intimidation).

³⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, Extraordinary, pt. II, sec. 3(i), rr. 3–4 (Feb. 25, 2021) (as amended).

³¹ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

unlawful information arises on receipt of a court order or a notification by the appropriate government or its agency. The decision remains relevant because vague demands to take down contested content could result in the excessive suppression of lawful speech. The decision did not shield an intermediary from liability for its own independent unlawful acts.

V. COURTS' READING OF PRIVACY IN THE DIGITAL REALM

A. Justice K.S. Puttaswamy (Retd.) v. Union of India

The nine-judge Bench ruling in *Puttaswamy* lays the foundation of Indian privacy jurisprudence. It rejected the contention that privacy could not be claimed as a constitutional right because it is not specifically named as such. What makes the decision relevant to cybercrime is that it links privacy to dignity, personal integrity and individual liberty.³² It provides a constitutional lens for examining the collection, transfer and processing of personal data as well as surveillance powers. However, *Puttaswamy* does not lay down a complete code of offences relating to privacy violations. Its constitutional value lies in the benchmark it provides for judging State interference and in shaping the law of privacy.

B. People's Union for Civil Liberties v. Union of India

In *People's Union for Civil Liberties v. Union of India*, the Supreme Court examined telephone tapping and its effect on privacy and free speech. The judgment acknowledged the gravity of unauthorised tapping and laid down procedural safeguards for the exercise of the power of interception.³³ The case remains pertinent in an age when surveillance can disclose email traffic, locations and associations. It underscores the need for surveillance powers to be exercised lawfully and to be safeguarded against abuse. The judgment does not require that all interception be treated as unlawful; the lawfulness of each measure is determined by reference to its statutory authority, its purpose and the controls that regulate it.

C. R. Rajagopal v. State of Tamil Nadu

In *R. Rajagopal v. State of Tamil Nadu*, the Court considered privacy in the context of the publication of personal information and the freedom of the press.³⁴ The judgment acknowledged that privacy and expression may conflict and identified situations in which personal information may be published. The case is relevant to the digital context because online publication is likely to increase both the scope of the privacy injury and the chance that the material remains available indefinitely. Nonetheless, privacy should not be understood as an absolute privilege

³² *Puttaswamy*, *supra* note 1.

³³ *People's Union for Civil Liberties*, *supra* note 11.

³⁴ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

to prevent all disclosures about oneself. The case shows that a clear line must be drawn between legitimate reporting in the public interest and the malicious leaking, posting or dissemination of private information.

D. *K.S. Puttaswamy v. Union of India* (Aadhaar judgment)

In the Aadhaar judgment, *K.S. Puttaswamy v. Union of India*, the Supreme Court examined the constitutional validity of aspects of the Aadhaar framework, including the collection and use of biometric and demographic information. The judgment considered data collection, privacy, State objectives and safeguards.³⁵ It is useful because of the implications and risks of large-scale identity systems. Such systems can serve administrative and service-delivery functions, but linked and cross-referenced databases pose risks if they are not subject to access controls, purpose limitation and accountability. The decision does not mean that digital identification systems are unlawful. It shows that the legal considerations governing the collection and use of personal data depend on the legal framework and safeguards of each system.

E. *Anuradha Bhasin v. Union of India*

In *Anuradha Bhasin*, the Court reviewed restrictions on internet services and their implications for constitutional freedoms. The Court held that restrictions must meet legal standards and directed that orders restricting the internet be published. The case matters because internet access is a vehicle through which other rights, including the freedom of expression, are enjoyed. Restrictions may in appropriate circumstances be necessary for the enforcement of cybercrime laws, but their scope may affect lawful and plainly non-offending users. The judgment favours measures that are rational, tailored and open to scrutiny over measures that are over-broad for their purpose.³⁶

F. Pegasus spyware proceedings

Questions of surveillance, privacy, national security and independent oversight were discussed in the Supreme Court proceedings concerning the Pegasus spyware. By an order dated 27 October 2021, the Supreme Court constituted a technical committee,³⁷ overseen by a former judge of the Supreme Court, to inquire into the allegations. Depending on the technology and the method of installation, spyware may allow access to communications, data files and device functions. The possibility of intrusion into personal and professional life raises major questions of legality, accountability and redress.

³⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 (Aadhaar).

³⁶ *Anuradha Bhasin*, *supra* note 13.

³⁷ *Manohar Lal Sharma v. Union of India*, 2021 SCC OnLine SC 985 (order dated Oct. 27, 2021).

The significance of the proceedings should be recorded precisely. Constituting a committee of inquiry did not mean that every allegation had been conclusively proved, or that any particular actor had used spyware unlawfully.³⁸ The proceedings instead show that urgent technical examination and credible investigation are needed when grave suspicions of spying are raised. They also reveal an institutional challenge: for the affected parties, it may be hard to establish what has happened when the relevant technical evidence is in the control of State agencies, vendors or foreign actors. Independent expertise and transparent processes are therefore necessary for accountability.

VI. NEW RISKS TO PRIVACY IN THE DIGITAL WORLD

A. Identity theft and financial cybercrime

Identity theft involves the unauthorised use of personal credentials or information to pose as another person in order to obtain services or financial benefits. The impact is not only financial. Victims may have their personal communications accessed without permission, suffer damage to their reputation and face difficulty in rectifying inaccurate records. Compromised data may be exploited on multiple other sites, compounding the harm.³⁹ Sections 66C and 66D of the IT Act may apply to identity theft and cheating by personation, depending on the facts. Secure authentication, prompt account recovery, the preservation of digital evidence and accessible complaint mechanisms are essential safeguards.

B. Cyberstalking and digital harassment

Cyberstalking can consist of continual unwelcome messaging and threats, following a person online, tracking their location or otherwise using their information to threaten and harass them. The impact can be worse where the perpetrator combines social-media information, public records and illegally obtained data. Section 78 of the BNS may apply when the statutory conditions for stalking, including targeted monitoring of electronic communications, are met.⁴⁰ Other provisions may be invoked depending on the conduct. Enforcement must, however, respect the freedom to communicate, criticise and observe. Over-broad enforcement can chill legitimate expression; weak enforcement leaves victims without protection. Enforcement must take context into account, applying the statutory criteria to the conduct alleged.⁴¹

³⁸ *Id.*

³⁹ *Sharat Babu Digumarti v. Govt. of NCT of Delhi*, (2017) 2 SCC 18.

⁴⁰ *Bharatiya Nyaya Sanhita*, *supra* note 27, § 78.

⁴¹ *Kalandi Charan Lenka v. State of Odisha*, 2017 SCC OnLine Ori 52.

C. Non-consensual intimate imagery and deepfakes

The sharing of private sexual images without consent, commonly called ‘revenge porn’, is an invasion of privacy and dignity. Digital media can magnify the damage through rapid sharing, accounts that are hard to trace and copies that never expire. Victims risk threats, blackmail, reputational damage and social exclusion. Section 66E of the IT Act covers a specific class of private-area images. Additional provisions may be relevant where the image is sexually explicit, where extortion or threats are involved, and where other statutory requirements are met.⁴²

Synthetic intimacy and deepfakes add further complications for the law. Synthetic images may show a person in a situation that never occurred, yet the reputational and mental-health harm may still be severe. In February 2026 the Central Government amended the Intermediary Rules to address synthetically generated information, requiring intermediaries, among other things, to label permissible AI-generated content clearly and to attach traceable metadata to it.⁴³ Existing legal frameworks nonetheless need to be reviewed thoroughly to determine whether they apply appropriately to synthetic content without expanding the reach of the criminal law beyond the words of the statute. Any intervention must be explicit about what conduct is forbidden, what constitutes consent and what mental element is required. It should also provide mechanisms for the redress of harm, while guarding against the wrongful removal of bona fide speech.

D. Data breaches and unauthorised disclosure

Data breaches may involve the disclosure of personally identifiable information, including identification details, financial data, medical information, authentication data or private messages.⁴⁴ A breach may result from hacking, employee malfeasance, accidental disclosure or poor system architecture. Each of these scenarios is treated differently in law and need not have the same consequences.

Criminal liability may attach where a person obtains or discloses information unlawfully. For breaches of duty by an organisation, there may be compensation or regulatory consequences. The legal analysis must specify the conduct, the duty and the statutory requirements. Section 43A of the IT Act remains in force as of October 2026, and its omission is scheduled for 13 May 2027.⁴⁵ The DPDP regime is significant for the future of personal-data regulation, but its

⁴² *Nipun Saxena v. Union of India*, (2019) 2 SCC 703.

⁴³ Press Release, MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, *Government Strengthens Regulatory Framework to Address AI-Generated Deepfakes*, Press Information Bureau (Aug. 6, 2026), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2295500> [hereinafter Deepfakes Press Release].

⁴⁴ Information Technology Act, *supra* note 3, §§ 43, 43A, 72, 72A.

⁴⁵ Digital Personal Data Protection Act, *supra* note 4, § 44(2); Commencement Notification, *supra* note 23.

commencement dates must be given due consideration. A careful legal analysis cannot treat obligations that have not yet commenced as if they were already in force.

E. Artificial intelligence and automated surveillance

Artificial intelligence can assist in detecting fraud and in monitoring cyber-threats and unusual transaction activity. It can also be used for facial recognition, behavioural analysis and continuous monitoring. 'Unauthorised' access is not the only source of privacy risk. Excessive or opaque processing can cause an individual to be placed on a suspicion list, refused a service or subjected to unusual scrutiny without explanation. The key questions concern the purpose of the processing and the data collected.⁴⁶ A distinction must be drawn between legitimate security processing and unwarranted State surveillance. How the DPDP framework is administered in future will bear on the governance of digital data; until then, constitutional principles and the existing law are of more immediate importance.

VII. CRITICAL ANALYSIS: GAPS IN INDIA'S PRIVACY FRAMEWORK

A. Fragmentation of remedies

Privacy is protected by a patchwork of law and sectoral regulation: constitutional law, the IT Act, criminal law, sectoral guidelines and the new DPDP structure. Each is designed for a different purpose, but their interplay can be complex for victims and institutions. One incident may involve all of them: unauthorised access, attempted identity theft, disclosure of sensitive information and failure to follow reasonable security practices. The victim may seek criminal, compensatory or regulatory redress,⁴⁷ each requiring a different process and standard of proof. The problem is not that there are many laws; it is that how they relate to one another may be unclear in practice. Clearer guidance and better procedural coordination are needed so that the multiplicity of laws produces proper protection.

B. The gap between constitutional recognition and practical application

The fact that privacy is a fundamental right does not mean that victims obtain real remedies in time. Victims may find it difficult to locate the perpetrator, collect digital evidence, have harmful content removed or seek redress when the data is stored elsewhere. Delay is especially harmful in cases of intimate images, impersonation or cyberstalking.⁴⁸ Data can be copied before legal proceedings begin, and privacy is then almost impossible to restore fully. A rights-based framework must therefore address institutional capacity, the preservation of evidence,

⁴⁶ Deepfakes Press Release, *supra* note 43.

⁴⁷ Digital Personal Data Protection Act, *supra* note 4, § 44(2); Commencement Notification, *supra* note 23.

⁴⁸ *Lalita Kumari v. Government of Uttar Pradesh*, (2014) 2 SCC 1.

complaint mechanisms and victim support. Formal legal recognition must be accompanied by processes able to keep pace with the speed and scale of digital harm.⁴⁹

C. Surveillance and disproportionate enforcement

Obtaining access to devices, communications or account information for a cybercrime investigation may be entirely justified. But it can reveal information unconnected with the crime and affect other people. It is not acceptable to argue in the abstract that surveillance enhances security and that every powerful technique is therefore beyond scrutiny.⁵⁰ To weigh security against privacy, the legal basis, aims, limits, proportionality and safeguards of each technique must be examined. Privacy is not, and never ought to be, a blanket prohibition. The right approach combines lawful investigative powers with proportionality, documentation, review and remedies⁵¹ against unlawful interference. Together these measures protect privacy while enabling legitimate criminal enforcement.

D. Corporate accountability

The way organisations gather and handle personal data determines how much of it is exposed to criminals. Poor access controls, excessive retention periods and weak security create risks for individuals. Nonetheless, the occurrence of a data breach should not be presumed to reveal a criminal offence. The legal response must distinguish between malfeasance, negligence, regulatory breach and incidents that occur despite appropriate controls. Corporate liability should rest on the existence of the relevant obligation and on proof, and sanctions should be proportionate to the proven violation.⁵² The DPDP framework aims to promote data governance, but its substantive provisions are being introduced gradually, and the compliance obligations currently in force must be identified carefully. Industry and individuals need regulatory certainty.

E. Privacy, expression and public interest

Privacy must be balanced against journalism, public accountability, research and legitimate law enforcement. Not every disclosure of personal information is unlawful, and not every restriction on disclosure is justified. The nature of the information, the manner of publication, the public interest, the expectation of privacy, the way the information was obtained and the relevant legal principles must all be taken into account.⁵³ This is especially so where personal information has

⁴⁹ Nipun Saxena, *supra* note 42.

⁵⁰ Manohar Lal Sharma, *supra* note 37.

⁵¹ *District Registrar & Collector v. Canara Bank*, (2005) 1 SCC 496.

⁵² Sharat Babu Digumarti, *supra* note 39.

⁵³ INDIA CONST. arts. 19(1)(a), 21.

been leaked and republished by many accounts. A proportionate legal system should neither treat privacy as a universal barrier to oversight nor accept that digital availability permits unrestricted collection or disclosure.

VIII. SUGGESTIONS FOR REFORM

A. Clarify the relationship between statutory regimes

Legal and institutional guidance should set out the relationship of the IT Act with the DPDP framework, the BNS and other sectoral laws. The different aims of criminal sanctions, compensation, data-protection duties and constitutional remedies should be delineated. Particular care is needed in the transition from Section 43A of the IT Act to the DPDP regime. Commencement dates need to be clearly communicated so that organisations and individuals can identify the applicable obligations and remedies.

B. Enhance protections for surveillance and digital searches

Monitoring and access to digital devices must rest on a legal basis and follow proportionate procedures. Legislation should limit the scope, duration and categories of information for which such authorisation is granted. Digital searches should, so far as reasonably possible and legally appropriate, limit the extent of unrelated personal information collected. A record should be kept of access, copying, retention and onward disclosure, and material unrelated to the investigation should be protected by law. Review procedures and remedies should be available where surveillance or access exceeds what the law permits. Emergency powers, where validly exercised, should still be accompanied by the relevant safeguards.

C. Improve victim support and reporting mechanisms

Victims need accessible ways to report identity theft, cyberstalking, intimate-image abuse and data breaches. Reporting pathways should enable evidence collection, referral to the appropriate authorities and notification of the available remedies. Complaint-handling systems should maintain confidentiality and keep any further disclosure of intimate material to a minimum. Where the complaint relates to intimate material, victims should not be subjected to avoidable repetition or circulation of their material in order to make the complaint. Training for police, prosecutors and judges should cover digital evidence, privacy-sensitive investigation and the distinction between unlawful conduct and protected expression.

D. Develop proportionate intermediary processes

Intermediaries should publish clear procedures for addressing complaints about wrongful sharing, impersonation and the abuse of intimate images. Any response should be grounded in

law, and directions should be legally valid and distinguishable from unsubstantiated claims. Transparency, reasoned decision-making and review processes can guard against both the under-removal and the over-removal of content. Intermediary protections should not amount to immunity for independent unlawful conduct, but platforms cannot be expected to wield unchecked investigative powers either.

E. Promote privacy by design and data minimisation

Businesses and other organisations can mitigate the impact of cyberattacks through data minimisation, access controls, strong authentication, suitable encryption of sensitive data, defined limits on data retention and regular security testing. Data should be collected only for legitimate purposes, and where there is no longer a need to process it for that purpose it should be deleted rather than kept indefinitely by default. Systems should allow the correction of inaccurate data and restrict access to confidential records.

F. Strengthen cross-border cooperation

Much cybercrime is committed through foreign websites and servers and involves cross-border financial transactions. Successful investigation of such cases requires cooperation with foreign authorities and service providers within the limits of the law. India must enhance its institutional capacity for the preservation of electronic evidence, the execution of legal requests and the international coordination of investigations. Transnational cooperation must respect jurisdictional limits, privacy rules and standards of fairness.

G. Strengthen privacy literacy and institutional accountability

Awareness campaigns can inform the public about the dangers of phishing, social engineering, weak account security, location sharing and the disclosure of personal information, and about how to report incidents and what legal action is available. Yet reliance on individual vigilance alone is insufficient. Businesses and public authorities must ensure suitable protective measures, and the authorities must investigate credible complaints robustly. Privacy literacy cannot substitute for institutional obligation.

IX. FINDINGS

First, the constitutional recognition of privacy in *Puttaswamy* offers a solid basis for guaranteeing informational autonomy, dignity and individual liberty. Yet constitutional recognition alone cannot guarantee privacy; effective legal remedies and institutional accountability are also required.

Second, the IT Act contains numerous provisions applicable to privacy-related cybercrime: Sections 43, 66, 66C, 66D, 66E, 72 and 72A. Each must be applied within its statutory scope and not as an overarching offence of privacy harm.

Third, the DPDP Act is an important step in data governance, but its phased commencement is legally significant. As of October 2026, the major substantive provisions are scheduled to commence on 13 May 2027, and Section 43A of the IT Act remains applicable until its scheduled omission on the same date.

Fourth, the decisions reviewed consistently affirm the need for legality, proportionality, procedural protections and independent review. The decisions on surveillance, the publication of personal data, restrictions on internet access and spyware allegations all turn on these considerations.

Fifth, the most pressing practical challenges relate to dispersed remedies, cross-border evidence, technological complexity, the limits of after-the-fact remedies, and the balance between effective investigation and privacy and other constitutional freedoms.

X. CONCLUSION

In India's digital society, the right to privacy is an indispensable component of dignity and autonomy. Cybercrime poses a grave threat to this right through identity theft, stalking, the abusive use of private images and videos, and other forms of data theft and profiling. India has significant constitutional and legal safeguards, but they will be effective only if law and policy are applied consistently. A proportionate model should rest on unambiguous legal obligations, transparent data processing, privacy-conscious investigation, straightforward victim remedies and checks against unwarranted surveillance. It must distinguish between deliberate criminal acts, the lawful use of technology and digital services that are exploited by others.

Ultimately, privacy and security are not mutually exclusive. Even 'rock-solid' security cannot provide a bulwark against wrongdoing without constitutional protections against arbitrary State and private interference. As India shapes its next legal response to cybercrime, the guiding principle should be the right balance between free thought, the rule of law and the democratic right to privacy.
