
RIGHT TO PRIVACY IN THE DIGITAL AGE: CONSTITUTIONAL CHALLENGES IN COMBATING CYBERCRIME IN INDIA

Pragya Agnihotri, Research Scholar, PhD, School of Legal Studies, Babu Banarasi Das University, Lucknow (India).

Prof. (Dr.) Sudhir Kumar Awasthi, Head, Department of Law, School of Legal Studies, Babu Banarasi Das University, Babu Banarasi Das University, Lucknow (India)

ABSTRACT

The digital revolution has transformed India into one of the world's largest digital economies, with nearly 958 million internet users. While this connectivity has driven economic growth and inclusion, it has also triggered an unprecedented surge in cybercrime—86,420 cases registered in 2023 and over 28 lakh complaints in 2025, causing financial losses exceeding ₹22,495 crore. Against this backdrop, the Supreme Court's landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) recognised the right to privacy as a fundamental right under Article 21, subject to the strict proportionality test. Yet, the Information Technology Act, 2000 (Sections 69 and 69A) and the Digital Personal Data Protection Act, 2023 continue to grant wide surveillance and data-access powers to the state, often with limited judicial oversight and broad national-security exemptions.

This paper critically examines the constitutional tensions between the right to privacy and the state's duty to combat cybercrime. It analyses the doctrinal evolution of privacy jurisprudence, the existing legal framework, major judicial interventions (including Shreya Singhal, Aadhaar, and Pegasus cases), and emerging challenges such as traceability mandates, encryption backdoors, and executive discretion. The study argues that while robust tools are necessary to fight cybercrime, the absence of independent oversight and proportionate safeguards risks eroding the very constitutional values the Puttaswamy judgment sought to protect. It concludes with recommendations for legislative and institutional reforms to strike a sustainable balance between privacy and security in the digital age.

Keywords: Right to Privacy, Cybercrime, Digital Age, Constitutional Challenges, Surveillance Powers, Data Protection, Proportionality Test, Information Technology Act, Judicial Review, India.

Introduction

The digital revolution has fundamentally reshaped India's socio-economic landscape, transforming it into one of the world's largest and most dynamic digital economies. Propelled by the Digital India initiative launched in 2015, the country witnessed an exponential surge in internet penetration. As of 2025, India boasts approximately 958 million active internet users, with over 57 per cent hailing from rural areas, marking an 8 per cent year-on-year growth.¹ This unprecedented connectivity has fostered economic opportunities, financial inclusion through digital payments, e-governance, and innovation in sectors ranging from fintech to artificial intelligence. Yet, it has concurrently engendered acute vulnerabilities, particularly in the realm of cybercrime and informational privacy.

Cybercrimes in India have escalated dramatically, encompassing hacking, phishing, identity theft, ransomware, and digital frauds. According to the National Crime Records Bureau (NCRB), 86,420 cybercrime cases were registered in 2023, reflecting a 31 per cent increase from the previous year.² The economic toll is staggering, with losses running into thousands of crores annually, compounded by low conviction rates and transnational dimensions of offences. High-profile incidents involving data breaches, Aadhaar-linked vulnerabilities, and state-sponsored surveillance tools like facial recognition technology and spyware have amplified public concern over the erosion of individual autonomy and dignity.³

Prior to 2017, the Indian Constitution lacked an explicit provision guaranteeing the right to privacy. Early judicial pronouncements in *M.P. Sharma v. Satish Chandra*⁴ and *Kharak Singh v. State of U.P.*⁵ adopted a restrictive view, refusing to recognise privacy as an independent fundamental right. Incremental protection emerged through linkages with Article 21 (right to life and personal liberty) and Article 19(1)(a) (freedom of speech and expression), but these remained fragmented. The seminal judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*⁶ marked a constitutional watershed. A unanimous nine-judge Bench of the Supreme Court declared the right to privacy as an intrinsic facet of Article 21, encompassing

¹ *India Internet 2025 Report*, Internet and Mobile Association of India (IAMAI), January 2026 (reporting 958 million active internet users as of 2025).

² National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Government of India, 2024) (noting 86,420 cybercrime cases, a 31 per cent rise from 2022)

³ Aditya Thakur, "The Right to Privacy in the Digital Age: Challenges and Legal Framework in India", *Indian Journal of Law and Public Policy* (2025).

⁴ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

⁵ *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.

⁶ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

informational, decisional, and bodily integrity dimensions. The Court prescribed a stringent proportionality test for any restriction: the existence of a law, a legitimate state aim, rational nexus, and minimal impairment.⁷

This judicial recognition coincided with the enactment of the Information Technology Act, 2000 (as amended in 2008) and the Digital Personal Data Protection Act, 2023 (with Rules notified in November 2025 and phased implementation underway). While these statutes empower law enforcement to combat cybercrime through provisions on interception, monitoring, and data processing (notably Sections 69 and 69A of the IT Act), they simultaneously raise profound constitutional dilemmas. Broad governmental exemptions under the DPDP Act for national security and crime prevention, coupled with limited judicial oversight on surveillance, risk disproportionate infringement of privacy rights.⁸

This paper examines the constitutional challenges inherent in balancing the right to privacy with the imperative of combating cybercrime in the digital age. It analyses the doctrinal evolution of privacy jurisprudence, critiques the existing legal framework, evaluates judicial interventions, and proposes reforms to ensure proportionality and accountability. Through a doctrinal and comparative lens, the study underscores the need for a rights-centric approach that upholds constitutional supremacy while addressing contemporary security threats.

I. Evolution of the Right to Privacy in India

The Indian Constitution does not contain an explicit provision guaranteeing the right to privacy. This constitutional silence initially led the Supreme Court to adopt a restrictive approach towards recognising privacy as a fundamental right. In its early jurisprudence, the Court was reluctant to read privacy into the existing fundamental rights. In *M.P. Sharma v. Satish Chandra*,⁹ a case concerning search and seizure, the Court held that there was no fundamental right to privacy as it was not explicitly enumerated in the Constitution. Similarly, in *Kharak Singh v. State of U.P.*,¹⁰ while the Court struck down certain police regulations authorising domiciliary visits as violative of Article 21, the majority opinion refused to recognise an

⁷ *Id.*, paras 297–319 (Chandrachud, J., for the plurality).

⁸ *The Digital Personal Data Protection Act, 2023* (Act 22 of 2023), s. 17; *The Information Technology Act, 2000* (Act 21 of 2000), ss. 69, 69A.

⁹ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

¹⁰ *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.

independent right to privacy.

A significant shift occurred in *Gobind v. State of M.P.*,¹¹ where the Supreme Court, for the first time, positively acknowledged that the right to privacy flows from the right to personal liberty under Article 21 and the freedoms under Article 19. Justice K.K. Mathew, speaking for the Court, referred to the American concept of the ‘right to be let alone’ and held that privacy-dignity claims deserve protection, subject to a compelling state interest test. This evolutionary trajectory continued in *R. Rajagopal v. State of T.N.*,¹² (popularly known as the Auto Shankar case), where the Court recognised the right to privacy against unauthorised publication of personal information, balancing it with freedom of the press under Article 19(1)(a).

The Court further strengthened privacy safeguards in *People’s Union for Civil Liberties (PUCL) v. Union of India*,¹³ a case concerning telephone tapping under the Indian Telegraph Act, 1885. It laid down detailed guidelines for interception of communications, affirming that any infringement of privacy must be backed by law, pursue a legitimate aim, and satisfy the test of proportionality.

The landmark turning point in the evolution of privacy jurisprudence came with the nine-judge Bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.¹⁴ Delivered on 24 August 2017, the Supreme Court unanimously declared the right to privacy as a fundamental right intrinsic to Article 21 (right to life and personal liberty) and also protected under Articles 19 and 14. The Court explicitly overruled the earlier observations in *M.P. Sharma* and *Kharak Singh* to the extent they denied the existence of the right to privacy. The judgment expansively defined privacy as encompassing informational privacy, decisional autonomy, and bodily integrity. Most importantly, it laid down a four-fold proportionality test for any restriction on the right to privacy: (i) the action must be sanctioned by law; (ii) it must pursue a legitimate state aim; (iii) there must be a rational nexus between the object and the means; and (iv) the means adopted must be necessary and proportionate with minimal impairment of the right.¹⁵

This judgment has become the constitutional bedrock for evaluating all state actions affecting privacy in the digital age, including surveillance, data protection, and measures for combating

¹¹ *Gobind v. State of M.P.*, (1975) 2 SCC 148.

¹² *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632

¹³ *People’s Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.

¹⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

¹⁵ *Ibid.*, paras 297-319 (per Dr. D.Y. Chandrachud, J.).

cybercrime.

II. The Landscape of Cybercrime in India

India's rapid digital transformation, symbolised by the Digital India initiative and the widespread adoption of digital payment systems such as UPI, has created an expansive digital ecosystem that cybercriminals are increasingly exploiting. With approximately 958 million active internet users as of 2025, the country offers a vast and often vulnerable attack surface.¹⁶

Official statistics from the National Crime Records Bureau (NCRB) indicate that 86,420 cases of cybercrime were registered in 2023, reflecting a 31.2 per cent increase from 65,893 cases in 2022.¹⁷ Financial frauds dominated these registered cases, constituting nearly 69 per cent of the total.¹⁸ However, the true scale of the problem is far greater when viewed through citizen-reported data. According to the Ministry of Home Affairs, over 28.15 lakh cybercrime complaints were received through the National Cybercrime Reporting Portal and related platforms in 2025, resulting in financial losses of ₹22,495 crore.¹⁹ This marked a nearly 24 per cent rise in reported cases from the previous year.²⁰

The landscape of cybercrime in India is both diverse and evolving. Predominant categories include investment and trading scams, "digital arrest" frauds (where perpetrators impersonate law enforcement officials), phishing, smishing, vishing, SIM swap frauds, identity theft, hacking, cyber stalking, online sexual harassment, and the dissemination of morphed or obscene material.²¹ Emerging threats have further complicated the scenario. The misuse of artificial intelligence for generating deepfakes, voice cloning for impersonation, and ransomware attacks targeting individuals and organisations have become increasingly common. Organised cybercrime syndicates, many operating transnationally, exploit encrypted communication tools, mule accounts, and cryptocurrency to evade detection.²²

Several structural and socio-economic factors exacerbate the vulnerability. Low levels of

¹⁶ India Internet 2025 Report, Internet and Mobile Association of India (IAMAI) (January 2026).

¹⁷ National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Government of India, 2025).

¹⁸ *Id.*

¹⁹ Ministry of Home Affairs, Government of India, data on cybercrime complaints and financial losses (2025), as reported in official releases.

²⁰ *Id.*

²¹ National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Government of India, 2025).

²² *India Cyber Threat Report 2025*, Data Security Council of India (DSCI).

cybersecurity awareness, particularly among rural and elderly populations, inadequate forensic infrastructure in several states, low conviction rates (often below 5 per cent), and delays in international cooperation through mutual legal assistance treaties continue to hinder effective enforcement.²³ The increasing linkage of critical services with digital identities such as Aadhaar has also heightened the risks associated with data breaches and mass surveillance.²⁴

This pervasive cybercrime ecosystem not only inflicts substantial economic damage and personal distress but also creates a compelling justification for the State to invoke surveillance, interception, and data-access powers. At the same time, it intensifies the constitutional tension between protecting the fundamental right to privacy—recognised in *Justice K.S. Puttaswamy (Retd.) v. Union of India*—and the legitimate imperative of ensuring public order and national security.

III. Legal Framework for Combating Cybercrime and Data Protection

The principal legislation governing cybercrime in India remains the Information Technology Act, 2000 (hereinafter “IT Act”), which was enacted to provide legal recognition to electronic records and digital signatures and was comprehensively amended by the Information Technology (Amendment) Act, 2008 to address emerging cyber threats.²⁵ Chapter XI of the IT Act enumerates specific cyber offences, including unauthorised access and hacking (Section 66), cheating by personation using computer resource (Section 66D), identity theft (Section 66C), violation of privacy by capturing or transmitting private images (Section 66E), and cyber terrorism (Section 66F).²⁶ These provisions are complemented by the newly enacted Bharatiya Nyaya Sanhita, 2023 (BNS), which replaced the Indian Penal Code, 1860, and incorporates digital offences such as forgery of electronic records (Section 336), criminal breach of trust involving digital assets, and cheating by impersonation in the digital domain.²⁷

For the purposes of surveillance and investigation, the IT Act confers extensive powers on the Central Government and authorised agencies. Section 69 authorises interception, monitoring, or decryption of any information generated, transmitted, or received in any computer resource

²³ Id.

²⁴ Aditya Thakur, “The Right to Privacy in the Digital Age: Challenges and Legal Framework in India”, *Indian Journal of Law and Public Policy* (2025).

²⁵ The Information Technology Act, 2000 (Act 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008 (Act 10 of 2009).

²⁶ Ibid., ss. 66, 66C, 66D, 66E and 66F.

²⁷ The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 336, 316 and 318.

in the interest of sovereignty and integrity of India, defence of India, security of the State, public order, or prevention of incitement to the commission of any cognisable offence.²⁸ Section 69A empowers blocking of access to any information through any computer resource on similar grounds, while Section 69B permits monitoring and collection of traffic data.²⁹ These powers are exercised through executive orders and are supported by the procedural framework under Section 5(2) of the Indian Telegraph Act, 1885, which permits interception of messages in the interests of public emergency or public safety.³⁰ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 further mandate significant social media intermediaries to enable traceability of originators of messages and to assist law enforcement agencies, though these provisions have been subjected to constitutional scrutiny for potential overbreadth.³¹

The Digital Personal Data Protection Act, 2023 (DPDP Act) marks India's first comprehensive data protection legislation. Notified in August 2023, the Act received its Rules in November 2025 and is being implemented in a phased manner.³² It adopts a consent-based framework for processing of personal data, recognises rights of the data principal (including access, correction, erasure, and grievance redressal), and imposes obligations on data fiduciaries regarding purpose limitation, data minimisation, and security safeguards.³³ The Act establishes the Data Protection Board of India as the regulatory authority. However, Section 17 provides broad exemptions to the Central Government and its agencies for processing personal data in the interests of sovereignty, integrity, security of the State, public order, or prevention of offences, thereby creating significant carve-outs that have been criticised for diluting privacy protections.³⁴

The framework is further strengthened by the role of the Indian Computer Emergency Response Team (CERT-In) under the IT Act, which issues directions on cybersecurity incidents, vulnerability reporting, and data localisation for critical sectors.³⁵ While these laws

²⁸ The Information Technology Act, 2000, s. 69.

²⁹ Ibid., ss. 69A and 69B.

³⁰ The Indian Telegraph Act, 1885 (Act 13 of 1885), s. 5(2).

³¹ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2) and r. 5(2).

³² The Digital Personal Data Protection Act, 2023 (Act 22 of 2023); Digital Personal Data Protection Rules, 2025 (notified 14 November 2025).

³³ Ibid., ss. 4–8, 12–15 and 20.

³⁴ Ibid., s. 17.

³⁵ The Information Technology Act, 2000, s. 70B; CERT-In Directions dated 28 April 2022 and subsequent notifications.

collectively equip law enforcement to combat cybercrime, they simultaneously raise constitutional concerns regarding proportionality and judicial oversight in light of the *Puttaswamy* proportionality test, particularly where surveillance powers operate with minimal prior judicial scrutiny and broad executive discretion.³⁶

IV. Constitutional Challenges: Balancing Privacy and Security

The real test for any democracy in the digital age is whether it can protect its citizens from cybercriminals without trampling on their basic right to privacy. India's Supreme Court drew a clear line in the 2017 *Puttaswamy* judgment: privacy is not an optional extra but a fundamental part of the right to life and personal liberty under Article 21 of the Constitution. Any government action that touches this right must clear a strict four-part test – it must be backed by law, serve a legitimate purpose, have a rational link to that purpose, and cause the least possible harm to privacy.³⁷ Yet, when we look at the laws meant to fight cybercrime, this balance often feels more like a tightrope walk.

The biggest flashpoints are the sweeping surveillance powers under Sections 69 and 69A of the Information Technology Act, 2000. These sections let authorised agencies intercept, monitor, or decrypt almost any digital communication – emails, chats, social media posts – on fairly wide grounds such as “public order” or “prevention of cognisable offences.” The decision usually rests with the executive, and prior judicial approval is not mandatory in most cases.³⁸ While these tools are undoubtedly useful for tracking organised fraudsters or terrorists, critics point out that the lack of independent oversight makes misuse all too easy. Once surveillance begins, it is hard for ordinary citizens to even know it is happening, let alone challenge it in court.

The Digital Personal Data Protection Act, 2023 adds another layer of worry. On paper, the law promises strong consent-based protections and rights for individuals. In practice, however, Section 17 gives the Central Government and its agencies broad exemptions whenever “sovereignty and integrity of India,” national security, or prevention of crime are involved.³⁹ These carve-outs are so wide that they risk turning the data-protection law into a shield for the state rather than a safeguard for citizens. When the same government that collects and processes

³⁶ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, paras 297–319.

³⁷ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, paras 297–319.

³⁸ The Information Technology Act, 2000, ss. 69 and 69A.

³⁹ The Digital Personal Data Protection Act, 2023, s. 17.

personal data also enjoys almost blanket immunity, the promise of accountability starts to look hollow.

The 2021 Intermediary Guidelines Rules have intensified the debate. They require major social media platforms to trace the “first originator” of messages and hand over user data to law enforcement on demand. There have also been repeated calls for “encryption backdoors” so that authorities can read end-to-end encrypted chats. While the intention is to help investigations, weakening encryption could open the door for hackers, foreign governments, and even rogue officials to snoop on millions of innocent users.⁴⁰

The Pegasus spyware episode brought these concerns into the public eye. When reports emerged that the government may have used powerful spyware to target journalists, lawyers, and political opponents, the Supreme Court was forced to constitute a technical committee. The episode showed how easily surveillance tools can be turned against democratic voices, chilling free speech and violating privacy on a massive scale.⁴¹

At bottom, these issues raise serious constitutional questions under Articles 14 (equality before the law), 19 (freedom of speech and expression), and 21. Do the current rules genuinely meet the *Puttaswamy* test of “minimal impairment”? Are there smarter, less intrusive ways – such as mandatory judicial warrants, independent oversight bodies, or time-bound reviews – that could fight cybercrime without eroding the very rights the Constitution guarantees? Until these questions are answered with stronger safeguards, the battle against cybercrime risks becoming an excuse for unchecked state power in the digital realm.⁴²

V. Judicial Interventions and Landmark Decisions

The Supreme Court of India has emerged as the most important guardian of the right to privacy in the digital age, stepping in repeatedly to check executive overreach in surveillance and data-handling measures aimed at combating cybercrime. While the *Puttaswamy* judgment of 2017 provided the constitutional foundation, subsequent decisions have tested and refined that framework in real-world disputes involving the IT Act, intermediary rules, and the new data

⁴⁰ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2).

⁴¹ *Manohar Lal Sharma v. Union of India* (Pegasus Spyware Case), Writ Petition (C) No. 1031 of 2021 (Supreme Court).

⁴² See generally, Snigdho Dhar, “The Right to Privacy in the Digital Age: A Constitutional Perspective” JLRJS (2025).

protection regime.

One of the earliest and most impactful interventions came in *Shreya Singhal v. Union of India*,⁴³ where the Court struck down Section 66A of the Information Technology Act, 2000 in its entirety. The provision, which criminalised the sending of “offensive” or “annoying” messages through computer resources, was held to be unconstitutionally vague and overbroad. It violated Articles 19(1)(a) and 21 by creating a chilling effect on free speech and indirectly undermining informational privacy. The judgment emphasised that any restriction on online expression must be narrowly tailored and cannot leave citizens in fear of arbitrary prosecution.

The proportionality test articulated in *Justice K.S. Puttaswamy (Retd.) v. Union of India* was soon applied to large-scale state data-collection projects. In the Aadhaar case (*Puttaswamy II*),⁴⁴ a five-judge Bench upheld the constitutional validity of the Aadhaar Act with important safeguards. The Court struck down provisions that allowed private entities to mandate Aadhaar linkage and those permitting sharing of biometric data with private parties, holding that such measures failed the test of minimal impairment. However, it permitted limited use of Aadhaar for welfare schemes and national security, subject to strict data-protection norms. This ruling underscored that even legitimate goals like preventing cyber-enabled welfare fraud cannot justify blanket erosion of privacy.

The Pegasus spyware controversy brought the tension between national security and privacy into sharp public focus. In *Manohar Lal Sharma v. Union of India*,⁴⁵ petitions alleged that the government had used Israeli-origin Pegasus spyware to target journalists, activists, lawyers, and opposition leaders. The Supreme Court constituted an independent technical committee to examine the claims. While the committee confirmed the presence of malware in several examined devices, it could not conclusively establish the use of Pegasus due to the government’s refusal to cooperate fully. The Court directed the government to frame clearer guidelines on the use of such surveillance tools and emphasised that any deployment must satisfy the *Puttaswamy* proportionality test. The episode highlighted the dangers of opaque executive-led surveillance and the need for greater judicial oversight and transparency.

More recently, the Court has begun scrutinising the Digital Personal Data Protection Act, 2023

⁴³ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁴⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1.

⁴⁵ *Manohar Lal Sharma v. Union of India*, Writ Petition (Civil) No. 1031 of 2021 (Supreme Court) (Pegasus spyware case).

and its Rules. In March 2026, a three-judge Bench agreed to examine the definition of “personal data” under the DPDP regime, amid concerns that overly broad exemptions for state agencies could legalise disproportionate surveillance and undermine the right to information.⁴⁶ Petitions challenging the structural independence of the Data Protection Board and the wide national-security carve-outs under Section 17 are currently pending, with the Court signalling that executive discretion in data processing must still meet constitutional standards of necessity and proportionality.⁴⁷

Challenges to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021—particularly the traceability mandate under Rule 4(2)—have also reached the judiciary. Several High Courts heard petitions arguing that forcing intermediaries to break end-to-end encryption violates privacy and free speech. The Supreme Court transferred these matters to the Delhi High Court in 2024 to ensure consistency, and the litigation remains ongoing.⁴⁸

Through these interventions, the Supreme Court has consistently reaffirmed that the fight against cybercrime cannot become a licence for unchecked digital surveillance. Yet, the absence of final, binding rulings in several high-profile cases (Pegasus and DPDP challenges) and the slow pace of judicial processes continue to leave important gaps in protection. The judiciary’s role remains crucial in ensuring that legislative and executive measures stay within constitutional bounds.

VI. Recommendations

To resolve these challenges:

1. Amend surveillance laws to mandate prior judicial authorisation and periodic legislative review, aligning with proportionality.
2. Strengthen the Data Protection Board’s independence and empower it with suo motu investigative powers.

⁴⁶ *The Reporters’ Collective v. Union of India*, pending, Supreme Court, order dated 12 March 2026.

⁴⁷ See also, constitutional challenges to the *Digital Personal Data Protection Act, 2023* and Rules, 2025 (Supreme Court notices issued February 2026).

⁴⁸ Supreme Court of India, order dated 22 March 2024 transferring challenges to the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* to the Delhi High Court.

3. Introduce encryption safeguards and prohibit mandatory backdoors, consistent with international standards (e.g., GDPR principles).
4. Enhance digital literacy, public awareness campaigns, and victim redressal mechanisms.
5. Foster international cooperation via updated MLATs and harmonised data protection norms.
6. Conduct regular privacy impact assessments for emerging technologies like AI and biometrics.

Conclusion

The right to privacy in India's digital age stands at a delicate crossroads. The Supreme Court's landmark *Puttaswamy* judgment recognised privacy as a fundamental right under Article 21 and laid down a clear proportionality test to guide any restriction. Yet, the rapid rise of cybercrime, combined with expansive surveillance powers under the IT Act and broad exemptions in the Digital Personal Data Protection Act, 2023, continues to test this constitutional balance. While judicial interventions have checked some overreach, the absence of robust independent oversight, mandatory judicial warrants, and meaningful accountability mechanisms leaves the right to privacy vulnerable.

A rights-centric approach is urgently needed. Legislative reforms must ensure that tools to combat cybercrime remain proportionate, transparent, and subject to independent review. Only then can India secure both its citizens' dignity in the digital realm and the safety of its digital economy, upholding the constitutional promise of a just and democratic society.

Bibliography

1. Data Security Council of India (DSCI), *India Cyber Threat Report 2025*.
2. Dhar, Snigdho, "The Right to Privacy in the Digital Age: A Constitutional Perspective" *JLRJS* (2025).
3. Digital Personal Data Protection Rules, 2025 (notified 14 November 2025).
4. Internet and Mobile Association of India (IAMAI), *India Internet 2025 Report* (January 2026).
5. Ministry of Home Affairs, Government of India, data on cybercrime complaints and financial losses (2025).
6. Mohanty, Nitisha, "Right to Privacy in The Digital Age: Legal Challenges and Emerging Trends in India" *IJSET* (Vol. 13, Issue 4, 2025).
7. National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Government of India, 2025).
8. Thakur, Aditya, "The Right to Privacy in the Digital Age: Challenges and Legal Framework in India" *Indian Journal of Law and Public Policy* (2025).
9. The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).
10. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
11. The Indian Telegraph Act, 1885 (Act 13 of 1885).
12. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
13. The Information Technology Act, 2000 (Act 21 of 2000) (as amended by the Information Technology (Amendment) Act, 2008).