NAVIGATING THE DIGITAL LABYRINTH: PRIVACY PROTECTION AND CYBER CRIMES IN THE INDIAN LEGAL FRAMEWORK

Nishu Singh, Research Scholar, Bundelkhand University, Jhansi

Prof. LC Sahu, Bundelkhand College, Jhansi

ABSTRACT

The rapid expansion of the digital technologies has revolutionized the governance, business and communication in India that brings up some puzzling issues concerning privacy and cyber laws. Article 21 of the constitution acknowledging the right to privacy has enhanced privacy of individuals in the online world. Nevertheless, the growing cases of cyber-crimes like identity theft, hacking and web bullying reveals serious regulatory issues. Information Technology Act, 2000 is the law that has set the general structure in dealing with cyber offence, but limitations still rise in the changing digital landscape. The Digital Personal Data Protection Act, 2023 is one of the legislative initiatives to improve the data management and responsibility. At the same time, the powers of state surveillance and interception still create their constitutional controversy. In the current paper, the interaction between the jurisprudence of privacy and regulation of cyber-crimes in the Indian legal system is considered as well. It gives a critical appraisal on whether the current laws are working to ensure that technological progression, national security and fundamental rights are balanced. The paper posits that even though the judicial acknowledgement of privacy is forward looking, the implementation and legal backups need reinforcement.

Keywords: Privacy, Cyber Crime, Article 21, Information technology act 2000, Digital personal data protection act 2023, Surveillance, Data protection.

1. INTRODUCTION: DIGITAL TRANSFORMATION AND THE PRIVACY PARADIGM

The twenty first century has seen a surge in the digital technologies like never before, and hence the governance, commerce, communication, and social interaction are fundamentally changing in India. The swift infiltration of the internet, mobile phones, electronic money transfer systems and electronic government projects has provided a digital ecosystem that promotes efficiency and availability. The adoption of technology in the administration and delivery of services has increased faster in the government through government programs like the Digital India programme;[1] however, at the same time, the issue on informational privacy and data security has become more pronounced.

Personal data has become one of the economic and strategic assets in the digital environment. The gathering, processing and storage of data of the masses carried out by the state and non-governmental corporations has transformed the interaction between the citizen and the state. Compared to the old understanding of privacy that was a matter of physical invasion, in case of digital privacy, the issue is one of surveillance, profiling, aggregation of data and algorithmic decision making. The fact that people are easily defrauded and become victims of identity theft, financial fraud, cyber stalking, and unauthorized data disclosure highlights the pressing need to have a strong legal regulation.

The publicity of the right to privacy as a basic right in the constitution in Article 21 of the Constitution was a radical change in the Indian jurisprudence.[2] In Kharak Singh v. State of Uttar Pradesh, the Supreme Court had initially assumed a narrow interpretation of privacy,[3] however the historic case of Justice K.S. Puttaswamy (Retd.) v. Union of India[4] brought about a change in this limited approach to the concept of privacy, clearly stated that privacy is inherent in life and personal liberty. The Court stated that the informational self-determination and provided the principles of legality, necessity, and proportionality to examine the state action in respect to privacy. This conceptual evolution has turned into the foundation of assessing the digital surveillance and data protection efforts.

In tandem with the constitutional factors, the statutory regulation of cyber activities has taken

[1] Ministry of Electronics and Information Technology, Government of India, Digital India Programme (2015).
[2] The Constitution of India, 1950, art. 21.
[3] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

a new shape with Information Technology Act, 2000, criminalizing about certain cyber offences and offering limited protection to data security,[5] however, with the change in technology, there have been structural loopholes in enforcement and regulatory oversight. Legislative awareness of these challenges is manifested in the development of the extensive data protection law, which is the Digital Personal Data Protection Act, 2023.[6]

Therefore, the digital transformation of India has created a multifaceted privacy paradigm, i.e., the paradigm where innovation, national security, economic growth, and human rights have to be put in balance. The main issue is whether the current legal system is sufficient to help protect personal autonomy in a more data-driven community.

2. LITERATURE REVIEW

India has had a significant discourse of privacy that has been changed by both constitutional adjudication, legislative, and scholarly analysis of the issue. M.P Sharma v. Satish Chandra[7] was an early judicial debate on privacy and Kharak Singh v. State of Uttar Pradesh,[8] the Supreme Court took a limiting view of privacy rights. Later commentary in the academy though has condemned this limited view and claimed that as part of dignity and liberty, privacy would have to be acknowledged under Article 21.[9] The radical ruling in Justice K.S. Puttaswamy (Retd.). v. Union of India[10] has since spawned a lot of scholarly interest, especially in the area of informational privacy, decisional autonomy, and the doctrine of proportionality.

Article 21 has been analyzed by scholars like Upendra Baxi in terms of its expansion and its consequences to the human rights jurisprudence in India.[11] The constitutional basis of privacy and normative framework of the Puttaswamy judgment, particularly the importance of the concept of dignity and autonomy, have been critically analyzed by Gautam Bhatia.[12] There is also academic commentary concerning the Aadhaar litigation (K.S. Puttaswamy v. Union of India, 2018), which discusses the concept of data minimization, surveillance architecture and

[5] The Information Technology Act, 2000 (Act 21 of 2000).
[6] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[7] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
[8] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
[9] The Constitution of India, 1950, art. 21.
[10] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[11] Upendra Baxi, The Future of Human Rights (Oxford University Press, 3rd edn., 2008).
[12] Gautam Bhatia, Privacy in the Age of Surveillance: The Supreme Court's Puttaswamy Judgment (2017) 52(40) Economic & Political Weekly 36.

state authority.[13]

Concerning statutory regulation, the Information Technology Act, 2000, literature sheds light on its revolutionary aspect of criminalizing cyber-crime and its ineffectiveness in aiding to resolve the current data protection issues. The existence of a narrow interpretation of Section 43A and the lack of clarity as to the application of the intermediary liability under Section 79.[14] The enactment of the Digital Personal Data Protection Act, 2023 has resulted in yet another debate on the consent architecture, state exemptions, and forms of regulatory oversight.

Although the area is increasingly becoming scholarly, there are still gaps in the complete analysis of the intersection of privacy jurisprudence and the regulation of cyber-crimes. To a large extent, the literature considers constitutional privacy and cyber offences as independent entities. In a bid to seal that gap, this paper aims at assessing the issues of privacy protection and cyber-crimes under one analytical framework and putting the statutory developments in context with constitutional principles.

3. RESEARCH METHODOLOGY

This study will be a doctrinal and analytical study to look at privacy protection and cyber-crimes in the Indian legal system. This research is mostly founded on secondary literature such as constitutional texts, acts of parliament, court rulings, government publications and academic texts. The Constitution, including Article 21, is also the subject of the legislative analysis, and more specifically, statutory instruments, the Information Technology Act, 2000 (Act 21 of 2000) and the Digital Personal Data Protection Act, 2023 (Act 22 of 2023), will be examined.

The study also presents a case-law examination of significant Supreme Court decisions, especially Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) relating to aadhaar and digital surveillance to learn how the law of informational privacy has changed over the years. Analytical concepts of the doctrine of proportionality and the concepts of legality and necessity are used to determine the constitutional validity of state action which concerns the privacy.

The study also analyzes the current trends such as intermediary liability, encryption controversies, and cyber-criminal activities by critically analyzing the policy documents and

[13] K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1.
[14] The Information Technology Act, 2000 (Act 21 of 2000), ss. 43A & 79.

regulatory frameworks. The methodology itself is still qualitative and is used to bring together constitutional principles and statutory mechanisms to determine whether the current legal system has done a sufficient job to balance out privacy, technological progress and national security issues.

4. PROTECTING PRIVACY IN THE INFORMATION AGE

The meaning and understanding of privacy in India has been redefined basically by the digital age. In contrast to the classical problems of privacy that are based on physical intrusion, modern issues of privacy are due to mass data mining, algorithmic profiling, biometric identification, and state surveillance. The development of the digital infrastructure, including e-governance systems, the social media ecosystem, and so on, has increased the necessity of legal interventions that would protect the autonomy of information. Today, privacy is inseparably connected with such notions as dignity, identity, and personal liberty mostly because in a data-driven society, personal information is both an economic resource and a mechanism of governance. The Indian legal system of digital privacy has been developed by interpreting the Constitution and interfering with the statutes, which is an unceasing effort to reconcile individual rights with the interests of the technological progress and the national security.

4.1 Indians have a Long History of developing the Right to Privacy

The Indian experience of judicial privacy is a gradual shift towards denial to constitutional recognition. In M.P. Sharma v. Satish Chandra,[15] an eight judge bench of the Supreme Court noted that there was no express right to privacy in the Constitution at all, especially concerning search and seizure. This counter-measuring method was once again endorsed, but weakened to some degree, in Kharak Singh v. State of Uttar Pradesh,[16] in which the Court declared domiciliary visits by police unconstitutional but made no explicit declaration that privacy was a fundamental right.

Later rulings started broadening the meaning of Article 21. In Gobind v. State of Madhya Pradesh,[17] the Court recognized the fact that privacy might be traced in the right to personal liberty, though within reasonable limitations. Later, in R. Rajagopal v. State of Tamil Nadu,[18]

[15] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
[16] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
[17] Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
[18] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

the court realized the right to be left alone and security against unjustified publication of personal information.

It was unanimously determined that the constitutional status was certainly established in Justice K.S. Puttaswamy (Retd.). v. Union of India,[19] in which a nine judge Constitution Bench unanimously declared that the right to privacy is inherent in life and personal liberty under Article 21 ensured by Part III of the Constitution. In Kharak Singh, the court reversed M.P. Sharma case and the majority opinion, and made privacy a right. Notably, it established the doctrine of proportionality and a three-fold criterion, namely, legality, necessity, and proportionality, to challenge state action that violated privacy. This ruling represented a change in doctrine where constitutional backing on the safeguarding of privacy on the internet was given.

4.2 Legal Construction: Information Technology Act, 2000

The IT act of 2000 (Act 21 of 2000) is the main law of cyber-crime and electronic governance in India. Even though it was initially adopted to promote electronic business and digital signatures, it has over time developed to accommodate policies that pertain to privacy protection.

The compensation in section 43A is given in case a body corporate fails to adopt reasonable security practices, which leads to wrongful loss or gain as a result of negligence in the handling of sensitive personal data.[20] This is an early attempt to give a statutory treatment of data protection, but is only applied to corporate bodies and does not have a comprehensive architecture.

Section 66C and 66D criminalizes the identity theft and cheating by personation using computer resources respectively. Section 66E punishes breaching privacy by capturing, publishing, or transmitting images of personal parts without consent.[21] These sections have a direct bearing on cyber-crimes, which involve the informational privacy.

The provisions of Section 69, 69A and 69B authorize the Central Government to intercept, monitor and decrypt or block digital information in the interest of sovereignty, integrity,

[19] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[20] The Information Technology Act, 2000 (Act 21 of 2000), s. 43A.
[21] Ibid., ss. 66C, 66D & 66E.

defense, security of the State or public order.[22] Although they offer a statutory support in the areas of surveillance, they pose constitutional concerns about the element of proportionality and accountability. Critical analysis on Shreya Singhal v. Union of India,[23] affirmed Section 69A though with procedural protection.

Section 79 creates an intermediary liability and the so-called safe harbour protection to intermediaries should they exercise due diligence and follow instructions given by the government.[24] This is the basis of the regulation of social media platforms and balancing the accountability of the platform with freedom of speech.

IT Act still lacks a broad system of data protection and is sectoral and reactive despite these protective measures.

4.3 Data Protection Regime in India

Having acknowledged the shortcomings of the current framework, the Government came up with the Personal Data Protection Bill, 2019 which was later changed to the Data Protection Bill, 2021 based on the recommendations of the Justice B.N. Srikrishna Committee (2018),[25] which aimed to introduce principles of consent, limiting the scope of purpose, minimization of data, and the establishment of a Data Protection Authority. Nevertheless, its withdrawal in 2022 was because of concerns of wide state exemptions and compliance burdens.

Later on, the Parliament overturned the bill by passing the Digital Personal Data Protection Act, 2023 (Act 22 of 2023). It gives a voluntary framework on how to process digital personal data, acknowledges the rights of the data principals, and it even gives the Data Protection Board of India to enforce. It includes the lawful processing obligations, the data security protection, and notification of breaches. Nonetheless, the Act has sweeping exemptions of state instrumentalities on the grounds of sovereignty and societal order, and that is where the issues of proportionality and responsibility emerge.

In such a way, the data protection regime in India is characterized by the shift of the disjointed statutory protection by IT Act to the more organized legislative framework by the 2023 Act.

[22] Ibid., ss. 69, 69A & 69B.
[23] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[24] The Information Technology Act, 2000 (Act 21 of 2000), s. 79.
[25] Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).

The success of such regime will finally lie in the regulation independence, judiciary checks and balances, and true commitment to the constitutional stipulations as stated in the Puttaswamy.

5. CRIMES RELATING TO PRIVACY

In addition to increasing the connectivity and economic activity, the spread of digital technologies has led to new types of criminality, which pose a direct threat to personal privacy. Cyber-crimes that are related to privacy include accessing and using personal information and identity theft to online harassment and intrusive surveillance. Such crimes destroy the informational autonomy and reveal the structural vulnerability of enforcement procedures. Indian law discusses these types of offences under the Information Technology Act, 2000 (Act 21 of 2000) with certain reinforcements of the Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023) as well as judicial interpretation. The issue is on how to make sure the response of criminal law is proportional and at the same time discourages the abuse of digital platforms.

5.1 Cyber Crimes and Data Breaches

There has been an increase in cyber-crimes in the Indian digital ecosystem using data breaches. Unauthorized entry into computer systems, retrieval of sensitive personal information and sharing of information that is confidential give a direct implication on privacy rights. Section 43 of the Information Technology Act, 2000 offers civil liability in unauthorized access, downloading or extraction of data.[26] Section 66 transforms some acts of the same into criminal acts when done dishonestly or fraudulently.[27]

The section 43A is more focused on corporate negligence in ensuring the confidences of personal information and makes provision on compensation of wrongful loss or gain in case such negligence to take reasonable security measures has been carried out by body corporates.[28] The rising number of large-scale data breaches underscores the weaknesses in the capacity to enforce and the reporting systems.

In the case of Justice K.S. Puttaswamy (Retd.) v. Union of India,[29] the Supreme Court has acknowledged the informational privacy as an aspect of Article 21, thus legally supporting the

[26] The Information Technology Act, 2000 (Act 21 of 2000), s. 43.
[27] Ibid., s. 66.
[28] Ibid., s. 43A.
[29] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

necessity to protect data. However, the application of criminal prosecution under the IT Act tends to be problematic in its practicality, such as the jurisdiction problem and technical requirements of evidence.

5.2 Identity Theft and Online Harassment

One of the most direct infringements of online privacy is identity theft. Section 66C of the Information Technology Act criminalizes use of electronic signatures, passwords, or other unique identification markers fraudulently or dishonestly.[30] Section 66D criminalizes personation cheating through computer resources.[31]

Privacy and dignity are also involved in online harassment, cyber stalking, and non-consent sharing of intimate images. Section 66E is an offence against the deliberate capturing, publishing, or transmitting of pictures of a private region without authorization,[32] and under the Bharatiya Nyaya Sanhita, 2023, section 78 is the issue of stalking which also includes watching online activity of a woman.[33]

The legal acceptance of a right to be left alone in the case of R. Rajagopal v. Tamil Nadu[34] enhances legal redress on unauthorized publication of personal information. Nevertheless, there has been unequal enforcement, especially when the digital platform boundaries are across borders, and when the offenders are anonymous.

5.3 Surveillance and Interception: National Security vs. Privacies

Along the border between the rights of privacy and national security issues lies the problem of state surveillance. In Section 69, the Central Government is given the power to intercept, monitor or decrypt information as a matter of sovereignty, integrity, defense or even public order.[35] Sections 69A and 69B also give power to the Central Government to block online information or even traffic data monitoring.[36]

Although these powers are constitutional in nature, their application should be subject to

[30] The Information Technology Act, 2000 (Act 21 of 2000), s. 66C.
[31] Ibid., s. 66D.
[32] Ibid., s. 66E.
[33] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 78.
[34] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[35] The Information Technology Act, 2000 (Act 21 of 2000), s. 69.
[36] Ibid., ss. 69A & 69B.

constitutional protection. In Puttaswamy (2017), the Supreme Court highlighted that the limit on privacy should pass the legality, necessity, and proportionality tests.[37] Earlier, the court in People's Union for Civil Liberties v. Union of India,[38] established the procedural protection of telephone interception by the Telegraph Act, and highlighted the necessity of control and rational decisions.

Therefore, the law of surveillance is an expression of a continuous conflict between mass security and individual rights. The transparency, independent control, and compliance with proportionality is also necessary to curb the arbitrary invasion of the privacy of digital space.

6. EMERGING ISSUES AND CASE STUDIES

The accelerated rate of the digital communication channel and biometric governance systems development has created difficult legal issues that relate to privacy, encryption, and the accountability of the platform. The latest scandals reflect the conflict between technological advancement, the state and the constitutional liberties. The Indian judicial system has been requested to adjudicate more and more of these disputes especially when it comes to encrypted communication, biometric databases on identities as well as intermediary liability.

6.1 WhatsApp v. Union of India: Traceability and Encryption

The encryption and traceability controversy emerged in the limelight after the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which was under the Information Technology Act, 2000 (Act 21 of 2000). Rule 4(2) asks that significant social media intermediaries that provide the messaging services should also facilitate identification of the first originator of information at the request of the government or court order, as it contravenes the end-to-end encryption and infringes the right to privacy of users.[39] The traceability requirement under Rule 4(2) of the IT Rules, 2021 has been challenged before the Delhi High Court in WhatsApp LLC v. Union of India (Delhi High Court, pending),[40] has been questioned in WhatsApp LLC against the Delhi high court on the basis that it compromises the end-to-end encryption and undermines the right to the privacy of the user.

[37] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[38] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
[39] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2).
[40] WhatsApp LLC v. Union of India, W.P.(C) 3163/2021, Delhi High Court (pending).

WhatsApp has stated that it would be a violation of encryption architecture to compel the intermediary to trace the source of the messages, which would allow hacking the informational privacy of the article 21 as accepted in Justice K.S. Puttaswamy (Retd.). v. Union of India.[41] The Union Government on the other hand has justified the rule as a need to fight misinformation, terrorism and child sex abuse contents. The controversy raises a constitutional dilemma of whether traceability obligations meet the test of proportionality set in the Puttaswamy.

The result of such litigation is momentous in the determination of the boundaries of state authority in gaining access to encrypted communications and in delineating the boundaries of digital privacy in India.

6.2 Aadhaar and Data Privacy

Aadhaar project is one of the largest biometric identification projects in the world and it creates significant concerns on the issue of surveillance and data security. Aadhaar scheme was analyzed with constitutional validity in K.S. Puttaswamy (Aadhaar-5J.) v. Union of India.[42] Although the Supreme Court supported the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, it put significant restrictions on the data retention, utilization by the private sector, and obliged connectivity.

The Court utilized the proportionality criterion expressed in Puttaswamy (2017) and determined that the scheme was aimed at a valid goal of a state in assuring the delivery of specific welfare. Nonetheless, it quashed provisions authorizing the authentication of individuals by Aadhaar by private companies and placed a focus on minimization of data, as well as, purpose limitation. The decision demonstrates that the courts acknowledged that the balance between the biometric information collection and the informational self-determination and dignity had to be balanced.

Even with judicial protection, data security and centralized databases as well as the possible profiling are reasons of concern. The Aadhaar case is, therefore, at the heart of the interpretation of constitutional limits of the digital identity systems run by the state.

[41] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[42] K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1.

6.3 Social Media Sites and Intermediary Responsibility

The social media platforms act as the main facilities of expression and information sharing, but on the other hand, misinformation, hate speech, and privacy invasion occur. The Information Technology Act, 2000 offers intermediaries section 79 protection of conditional safe harbour to third-party content under the condition of due diligence.[43] Shreya Singhal v. Union of India, the Supreme Court made it clear that only in cases when a court order or a government notification is received by the intermediaries, the illegal content should be removed under Section 69A.[44]

The IT Rules 2021 increased the due diligence requirements such as redressal to grievances and compliance officers. These restrictive actions will help improve accountability on the platforms and still safeguard the freedom of expression as provided by Article 19(1) (a).[45] Nevertheless, the critics believe that broad executive authority and compliance costs can have an indirect impact on privacy and speech.

Together, these new issues depict the dynamic relationship between the constitutional rights, statutory regulation, and technological architecture. They emphasize the need to use proportionality, transparency, and independent control to make sure that digital governance structures do not undermine the basic privacy provisions.

7. PRIVACY AND NATIONAL SECURITY: THE PROPORTIONALITY DOCTRINE

Expansion of digital surveillance has heightened the constitutional controversy on individual privacy and national security. The state agencies in the age of digital technology have superior technical abilities to eavesdrop on communications, gather internet activity, and gather as much personal information as they wish. Even though these kinds of measures are usually explained by the principles of sovereignty, social order, and crime prevention, they directly involve defining the basic right to privacy as provided in Article 21 of the Constitution. The constitutional dilemma would be to make sure that the security measures do not turn into a tool of random invasions.

[43] The Information Technology Act, 2000 (Act 21 of 2000), s. 79.
[44] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[45] The Constitution of India, 1950, art. 19(1)(a).

The doctrine of proportionality has become the key constitutional instrument to the solution of this tension. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court unequivocally held that any limitation on privacy should be met with a structured test of proportionality.[46]

The Court established that state action should be able to address the following requirement, legality (presence of law), legitimate purpose, rational nexus, necessity, and procedural requirements to prevent abuse.

The proportionality is of significance to a certain extent in the surveillance laws like Section 69 of the Information Technology Act, 2000 where the government is permitted to intercept, monitor, or decrypt digital information in under given circumstances.[47] Despite the statutory support, constitutional support would be determined by the extent to which such powers are executed with proper safeguards, transparency and checks and balances. Earlier in, People's Union for Civil Liberties v. Union of India, the Supreme Court stated that procedural measures in telephone interception scenarios should be given due consideration since it is necessary to avoid irrational executive discretion.[48]

The proportionality doctrine is therefore a balance mechanism in the constitution. It is not in dispute of national security goals but requires any limitations on privacy to be limited and open to the review of a court. Proportionality is a mandatory requirement in the digital environment where surveillance technologies are not only ubiquitous but also obscure to maintain democratic accountability. Privacy and security are not a matter of complete preference of one over the other, but rather a matter of constitutional discipline that must see to it there is necessity, transparency, and the lowest intrusion.

8. CONCLUSION AND SUGGESTIONS

The history of privacy jurisprudence in India indicates that there was a massive constitutional change especially following the acknowledgement of privacy as an inherent right in Article 21. Although there has been an enhancement of normative protection because of judicial developments, the digital ecosystem remains a problem of complexity through the spread of

[46] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[47] The Information Technology Act, 2000 (Act 21 of 2000), s. 69.
[48] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

cyber-crimes, data breaches, encrypted communication, and broadening surveillance capabilities. Statutory provisions, such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, are quite a positive development; but it can be seen that organizational weaknesses in the enforcement, regulatory autonomy, and control systems are still present.

When it comes to a successful privacy protection, institutional accountability and transparency in the surveillance practices are to be enhanced. They should institutionalize independent review mechanisms and periodical auditing of interception orders that would be used to curb the abuse of executive power. Moreover, there should be more definite regulations about the intermediary liability and encryption requirements to prevent the excessive invasions into the digital communications. Enforcement would be effective when agencies involved in cyber-crime investigation and better data breach reporting mechanisms are involved in capacity-building.

Finally, the Indian system of digital governance can be sustained through the strict compliance with the doctrine of proportionality, strong judicial control, and the rights-oriented regulatory strategy. Striking the balance between innovation, national security, and individual autonomy needs to be refined with constant legislative ways that are in compliance with the values of the constitution.

Reference

1. Ministry of Electronics and Information Technology, Government of India, Digital India Programme (2015).
2. The Constitution of India, 1950, art. 21.
3. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
4. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
5. The Information Technology Act, 2000 (Act 21 of 2000).
6. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
7. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
8. Upendra Baxi, The Future of Human Rights (Oxford University Press, 3rd edn., 2008).
9. Gautam Bhatia, Privacy in the Age of Surveillance: The Supreme Court's Puttaswamy Judgment (2017) 52(40) Economic & Political Weekly 36.
10. K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1.
11. The Information Technology Act, 2000 (Act 21 of 2000), ss. 43A & 79.
12. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
13. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
14. The Information Technology Act, 2000 (Act 21 of 2000), ss. 66C, 66D & 66E.
15. The Information Technology Act, 2000 (Act 21 of 2000), ss. 69, 69A & 69B.
16. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
17. Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).

18. The Information Technology Act, 2000 (Act 21 of 2000), s. 43.

19. The Information Technology Act, 2000 (Act 21 of 2000), s. 66.

20. The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 78.

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

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

23. WhatsApp LLC v. Union of India, W.P.(C) 3163/2021, Delhi High Court (pending).

24. The Constitution of India, 1950, art. 19(1)(a).