Royal International Global Journal of Advance and Applied Research
Peer Reviewed International, Open Access Journal.
ISSN: 2998-4459 | Website: https://rlgjaar.com Volume-2, Issue-2 | February - 2025

Original Article

Surveillance and Data protection Laws: Compatibility with Articles 19 & 21

Milan Kishorebhai Gondaliya[1], Dr. Janki Thakkar[2]
[1]Research Scholar (Phd)
[2]Guide, Swaminarayan University
Residence: Chitaliya Road Akshar Dham Society -Jasdan

Manuscript ID:
RIGJAAR-2025-020203

ISSN: 2998-4459

Volume 2

Issue 2

Pp. 9-13

February 2025

Submitted: 10 Jan. 2025

Revised: 17 Jan. 2025

Accepted: 15 Feb. 2025

Published: 28 Feb. 2025

Correspondence Address:
Milan Kishorebhai Gondaliya, Research Scholar (Phd)
Email: - milangondaliya24@gmail.com

Quick Response Code:

Web. https://rlgjaar.com

DOI:
10.5281/zenodo.15533947

DOI Link:
https://zenodo.org/records/15533947

Abstract:-

The rapid advancements in technology have revolutionized surveillance practices and data management, raising critical concerns about privacy and individual freedoms. In India, Articles 19 and 21 of the Constitution guarantee fundamental rights. The growing reliance on surveillance systems and the collection of personal data by governments and private entities often results in conflicts with these constitutional rights. The research identifies gaps and challenges, including overbroad surveillance laws, lack of accountability, and inadequate safeguards against misuse of personal data. It highlights the need for a balanced approach that upholds national security while protecting individual rights. Recommendations include stricter data protection legislation, judicial oversight for surveillance activities, and increased public awareness.

This paper contributes to the discourse on privacy, technology, and human rights, aiming to ensure that surveillance and data protection laws evolve in alignment with constitutional principles, fostering a secure and rights-respecting digital ecosystem in India. It evaluates how these frameworks align or conflict with constitutional mandates, judicial pronouncements (notably the Puttaswamy judgment), and international human rights standards. Particular attention is paid to the balance between national security interests and individual privacy rights, the need for legal safeguards, oversight mechanisms, and the role of consent in data processing.

Through a doctrinal and comparative legal approach, the paper highlights gaps in transparency, accountability, and legal redress in the existing surveillance regime. It concludes with recommendations for ensuring that surveillance and data protection laws uphold constitutional freedoms, foster digital trust, and remain consistent with the spirit of Articles 19 and 21.

Keywords:- *Surveillance, Data Protection, Right to Privacy, Freedom of Expression, Digital Rights, Personal Liberty, Puttaswamy Judgment, Data Security, Information Technology Act, Digital Personal Data Protection Act 2023.*

Introduction:-

The digital age has ushered in unprecedented advancements in technology, transforming how individuals, organizations, and governments operate. Central to this transformation is the extensive use of surveillance systems and data collection practices aimed at ensuring national security, improving governance, and enhancing economic efficiency. However, this increasing reliance on surveillance and data-driven systems poses significant challenges to fundamental rights guaranteed under the Indian Constitution, particularly Articles 19 and 21. Article 19 ensures the right to freedom of speech and expression, which encompasses the right to communicate freely without undue interference. Surveillance mechanisms, particularly those involving mass data collection and interception of communication, can have a chilling effect on this freedom, deterring individuals from exercising their right to free expression. Similarly, Article 21 guarantees the right to life and personal liberty, which, as interpreted by the Supreme Court in K.S. Puttaswamy v. Union of India (2017), includes the right to privacy. The increasing encroachment on personal data through unregulated surveillance practices raises concerns about the violation of this fundamental right. This study delves into the compatibility of India's surveillance and data protection laws with the constitutional guarantees enshrined in Articles 19 and 21. along with recent developments like the Digital Personal Data Protection Act, 2023. It also explores judicial interventions that have attempted to balance the competing interests of state security and individual rights.

Methodology:-

This research adopts a doctrinal legal research methodology, focusing on the analysis of constitutional provisions, statutes, judicial decisions, and scholarly commentaries related to surveillance and data protection in India. The study aims to assess the compatibility of current surveillance practices and data protection laws with Articles 19 and 21 of the Constitution of India, which guarantee the right to freedom of speech and expression and the right to life and personal liberty, respectively.

How to cite this article:
Gondaliya, M. K., & Thakkar, J. (2025). Surveillance and Data protection Laws: Compatibility with Articles 19 & 21. Royal International Global Journal of Advance and Applied Research, 2(2), 9–13.
https://doi.org/10.5281/zenodo.15533947

Royal International Global Journal of Advance and Applied Research
Peer Reviewed International, Open Access Journal.
ISSN: 2998-4459 | Website: https://rlgjaar.com Volume-2, Issue-2 | February - 2025

1. Research Design
Qualitative in nature, relying on interpretation and critical analysis of legal texts.
Analytical and descriptive, aiming to explore and explain the legal landscape surrounding surveillance and data protection.
2. Sources of Data
Primary sources: Constitutional provisions, statutory laws (such as the Information Technology Act, 2000; the Indian Telegraph Act, 1885; and the Digital Personal Data Protection Act, 2023), and landmark judicial pronouncements (e.g., K.S. Puttaswamy v. Union of India).
Secondary sources: Books, journal articles, reports by law commissions and committees (such as the Justice B.N. Srikrishna Committee Report), academic commentaries, and relevant international legal instruments and comparative jurisprudence.
3. Scope of Study
The study covers Indian surveillance laws and practices, including governmental programs and their legal backing.
Analysis includes the Digital Personal Data Protection Act, 2023, and its implications on privacy and freedom of expression.
Comparative insights from other democratic jurisdictions are included for broader perspective.
4. Objectives
To examine the extent to which Indian surveillance and data protection laws align with constitutional rights under Articles 19 and 21.
To evaluate the judicial response and legal evolution of the right to privacy in India
To suggest reforms for making surveillance laws more transparent, accountable, and rights-compliant.
5. Limitations
The research does not include empirical data or field surveys.

Review of Literature:-
The issue of surveillance and data protection laws in the context of fundamental rights, particularly Articles 19 and 21 of the Indian Constitution has been widely debated across legal, academic, and policy domains. This review examines key contributions from judicial precedents, legislative frameworks, scholarly articles, and international practices to establish the foundation for this study.

Judicial Perspectives on Privacy and Freedom
Right to Privacy as a Fundamental Right
The landmark case of K.S. Puttaswamy v. Union of India (2017) recognized the right to privacy as intrinsic to the right to life and personal liberty under Article 21.The judgment emphasized that any infringement of privacy must pass the tests of legality, necessity, and proportionality. Scholars like Gautam Bhatia (2017) argue that while the judgment was progressive, its practical implementation remains a challenge due to outdated surveillance laws.

Surveillance and Free Speech
The Supreme Court in People's Union for Civil Liberties (PUCL) v. Union of India (1997) addressed issues of telephone tapping under the Indian Telegraph Act, 1885, highlighting its impact on Article 19(1)(a).The court held that surveillance without adequate safeguards could deter individuals from freely expressing themselves, thereby infringing upon their constitutional rights. Critics have noted that the safeguards prescribed, such as oversight by review committees, are insufficient to prevent misuse.
Legal Framework Governing Surveillance and Data Protection

Surveillance Laws in India
India's surveillance framework is primarily governed by the Indian Telegraph Act, 1885, and the Information Technology Act, 2000.Scholars like Usha Ramanathan (2011) argue that these laws grant excessive powers to the executive, with limited judicial or parliamentary oversight. The absence of a comprehensive surveillance law has led to opaque practices, particularly under programs like Central Monitoring System (CMS) and National Intelligence Grid (NATGRID).

Data Protection Laws
The introduction of the Digital Personal Data Protection Act, 2023, marked a significant step toward regulating data collection and usage. The law seeks to provide transparency and accountability in data processing while addressing individual rights. Scholars, including Vrinda Bhandari (2023), argue that the Act lacks provisions to regulate state surveillance and fails to provide adequate safeguards for sensitive data.

Impact of Surveillance on Articles 19 and 21
Chilling Effect on Free Speech
Research by Human Rights Watch (2020) highlights how pervasive surveillance practices can discourage individuals from expressing dissent, thus undermining Article 19(1)(a).Studies in surveillance-heavy regions have documented self-censorship among journalists, activists, and academics.

Privacy Violations and Discrimination
Studies by Privacy International (2019) emphasize that indiscriminate data collection disproportionately impacts marginalized communities, leading to potential violations of Article 21. The Aadhaar program has faced criticism for enabling mass surveillance and profiling, as noted by Anja Kovacs (2018).
International Comparisons
European Union
The General Data Protection Regulation (GDPR) provides robust safeguards against misuse of personal data while ensuring accountability for state surveillance. Scholars like Arindrajit Basu (2020) suggest that India can adopt GDPR-like principles to enhance its data protection.
United State
The U.S. PATRIOT Act (2001) expanded surveillance powers but faced criticism for violating constitutional rights. Balancing national security with individual freedoms requires transparent laws and effective oversight mechanisms.

Scholarly Debates
Balancing Security and Privacy
Legal theorists, including Alan Westin (1970), argue that privacy is a critical element of democratic societies. Scholars emphasize the need for proportional surveillance measures that respect individual rights.

Technological and Ethical Challenges
Authors like Shoshana Zuboff (2019) highlight the risks of "surveillance capitalism," where data collection serves both state and corporate interests. The lack of ethical safeguards in data collection exacerbates privacy concerns, as discussed by Pranesh Prakash (2020).

Data Analysis:-
The data analysis in this study involves a comprehensive examination of the legal frameworks governing surveillance and data protection in India, and their alignment with the constitutional provisions of

Royal International Global Journal of Advance and Applied Research
Peer Reviewed International, Open Access Journal.
ISSN: 2998-4459 | Website: https://rlgjaar.com Volume-2, Issue-2 | February - 2025

Articles 19 and 21. The analysis integrates case law, statutory provisions, scholarly commentary, and comparative insights to assess the compatibility of these laws with fundamental rights. This section presents a synthesis of the key findings based on the legal review, case studies, expert opinions, and comparative analysis.

Analysis of Legal Frameworks

Surveillance Laws in India

Indian Telegraph Act, 1885 and Information Technology Act, 2000:

These statutes provide the legal foundation for surveillance in India. However, they have been critiqued for lacking robust safeguards against potential abuse, as highlighted in various judicial rulings. While the Indian Telegraph Act permits interception of communications for reasons related to national security or public order, it does not offer clear limitations on the scope or duration of surveillance, which raises concerns under Articles 19 (freedom of expression) and 21 (right to privacy). The lack of judicial oversight and transparency in surveillance activities is a significant concern. Expert opinion, as discussed by Usha Ramanathan (2011), suggests that these laws allow for the exercise of broad surveillance powers without adequate checks, potentially infringing upon the constitutional guarantees of free speech and privacy.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, aims to provide data protection by regulating the collection, processing, and storage of personal data.While the law provides some level of protection for individuals by introducing principles of consent, purpose limitation, and data security, it still leaves room for the government to access personal data without sufficient accountability or safeguards. Critics argue that the law inadequately addresses concerns related to state surveillance and lacks provisions for meaningful judicial oversight. The Act permits the government to process personal data for reasons related to national security and public order, potentially conflicting with the constitutional right to privacy (Article 21) and freedom of expression (Article 19).

Judicial Interpretations and Compatibility with Articles 19 and 21

Right to Privacy and Surveillance

The Supreme Court in K.S. Puttaswamy v. Union of India (2017) affirmed that the right to privacy is protected under Article 21 of the Constitution. The judgment laid down that any infringement of privacy must satisfy the three-fold test of legality, necessity, and proportionality. Surveillance laws, as currently framed, do not always meet this test. In particular, the broad powers conferred on the executive by surveillance laws raise questions about the proportionality and necessity of such measures. The lack of clear legal guidelines on proportionality and necessity in the surveillance laws violates the constitutional protections guaranteed by Article 21. While surveillance may be justified in specific circumstances, without adequate safeguards, it can undermine privacy and individual freedoms.

Freedom of Speech and Expression

The surveillance mechanisms, if excessively broad or poorly regulated, can chill freedom of speech and expression, which is protected under Article 19(1)(a). In People's Union for Civil Liberties (PUCL) v. Union of India (1997), the Supreme Court ruled that unauthorized telephone tapping could impede the free expression of individuals.Expert commentary, such as that by Arvind Gupta (2020), emphasizes that unchecked surveillance systems can create a chilling effect, where individuals hesitate to express dissent or engage in free speech for fear of being monitored. This undermines the constitutional guarantee of free speech under Article 19.

Case Study Analysis

Aadhaar and Privacy Concerns

The Aadhaar program, which mandates biometric identification for accessing various services, has raised significant concerns regarding privacy. The Supreme Court in K.S. Puttaswamy (2017) ruled that while Aadhaar could be constitutionally valid, its use must be strictly regulated to prevent violations of privacy. The Court specifically flagged concerns related to data security and the potential for misuse of personal information. Despite the Court's ruling, implementation challenges persist, as the system's vulnerability to data breaches and its potential for surveillance remain significant. The data collected for Aadhaar can be used for surveillance purposes, undermining the protection of privacy under Article 21. There is an inherent tension between the objectives of public welfare and the safeguarding of privacy rights under the Indian Constitution.

Surveillance Programs: CMS and NATGRID

India's surveillance programs, such as the Central Monitoring System (CMS) and the National Intelligence Grid (NATGRID), have been under scrutiny for their potential to infringe upon privacy rights without sufficient checks. These programs operate with limited public transparency, raising concerns about the unregulated monitoring of citizens. The absence of a clear legal framework and independent oversight for these surveillance programs means that they could infringe upon both privacy (Article 21) and freedom of speech (Article 19), as individuals may be deterred from expressing themselves freely due to fear of surveillance.

International Comparisons

European Union (GDPR)

The General Data Protection Regulation (GDPR) provides a robust framework for protecting personal data and regulating state surveillance. The GDPR enshrines the right to privacy, with strict conditions for data processing, transparency, and accountability. India's legal framework, in comparison, is more permissive and lacks the stringent safeguards seen in the GDPR. The absence of specific regulations for surveillance practices in India leads to greater risks for potential abuse and privacy violations.

United States (PATRIOT Act)

The U.S. PATRIOT Act grants broad surveillance powers to the government but has been criticized for infringing upon individual rights. Critics argue that such expansive surveillance laws can lead to overreach and rights violations, as seen in the U.S. debates on privacy versus security. India's surveillance laws face similar criticisms regarding the balance between state security and individual freedoms. India can learn from the U.S. experience by ensuring stronger legal safeguards and judicial oversight.

Summary of Findings

The analysis reveals several key issues:

India's surveillance and data protection laws often fall short in safeguarding the rights to privacy (Article 21) and free expression (Article 19) Laws such as the Indian Telegraph Act and the Digital Personal Data Protection Act

Royal International Global Journal of Advance and Applied Research
Peer Reviewed International, Open Access Journal.
ISSN: 2998-4459 | Website: https://rlgjaar.com Volume-2, Issue-2 | February - 2025

allow for extensive data collection and surveillance, without sufficient limits or oversight. The study highlights the need for stronger judicial oversight and clearer legal standards to ensure that surveillance practices align with constitutional protections.

Recommendations:-

Strengthening Data Protection Laws

Clearer and Stricter Regulations:

The Digital Personal Data Protection Act, 2023, while a step forward, needs stronger provisions to protect against unauthorized data processing and surveillance. Clearer guidelines should be introduced regarding the scope of government access to personal data for national security and public order purposes.

Minimizing Government Access:

Provisions for government access to personal data should be narrowly tailored and require judicial oversight. The grounds for surveillance should be well-defined, and access to data should be subject to an independent review by a data protection authority or judiciary to ensure compliance with constitutional rights.

Judicial Oversight and Transparency in Surveillance Programs

Enhanced Judicial Scrutiny:

Surveillance programs like the Central Monitoring System (CMS) and National Intelligence Grid (NATGRID) should be subject to regular judicial scrutiny to ensure they are in compliance with constitutional rights. Surveillance orders must be reviewed by an independent judiciary, not just the executive, and must adhere to the principles of necessity and proportionality.

Public Accountability and Transparency:

There should be greater transparency regarding the scope and nature of surveillance activities undertaken by the state. Annual reports detailing the extent of surveillance, the number of interceptions, and the safeguards in place should be published and made accessible to the public to ensure accountability.

Independent Oversight Mechanisms:

Independent oversight bodies, such as a National Privacy Commission, should be established to monitor state surveillance programs and ensure they do not violate the right to privacy or freedom of expression. These bodies should have the power to issue binding decisions regarding surveillance practices.

Aligning Surveillance Laws with Constitutional Principles

Adherence to the Three-Fold Test:

Surveillance laws must align with the Supreme Court's three-fold test of legality, necessity, and proportionality, as established in K.S. Puttaswamy v. Union of India (2017). This requires that any surveillance measures must be legal, necessary to achieve a legitimate aim (such as national security), and proportionate to the harm they seek to prevent.

Revisiting Broad Powers in Existing Laws:

Existing laws like the Indian Telegraph Act, 1885 and the Information Technology Act, 2000 should be revisited and revised to ensure that surveillance powers are not excessively broad or vague. For example, surveillance provisions should limit data retention periods and specify the nature of the data that can be intercepted, ensuring they are proportionate to the intended goal.

Strengthening the Right to Privacy

Privacy as a Fundamental Right:

The legal framework must be developed with the understanding that privacy is a fundamental right, as enshrined by the Supreme Court in the Puttaswamy judgment. The government must prioritize privacy protections by ensuring that all surveillance measures, including data collection, processing, and storage, are compatible with the right to privacy under Article 21.

Clear Definitions of Consent and Data Collection: The law should require that all data collection, including for surveillance purposes, must be done with explicit consent from individuals. Any exceptions to this principle (for national security or public order) must be clearly outlined and subject to judicial review.

Promotion of Privacy Awareness and Civil Liberties

Public Education on Privacy Rights:

The government should promote public awareness about privacy rights and the legal protections available to individuals. Civil society organizations, universities, and other stakeholders should be involved in educating citizens about their rights under the Constitution, data protection laws, and how to exercise those rights in the context of state surveillance.

Empowering Whistleblowers: Mechanisms for whistleblowing should be introduced to allow individuals within government agencies to report instances of unlawful surveillance. This could help ensure accountability and transparency in state surveillance practices.

Balancing National Security with Individual Rights

National Security and Privacy Balance:

While national security is a legitimate concern, it is essential that the government adopts a balance between safeguarding security and protecting individual privacy rights. This can be achieved through proportionate and targeted surveillance, rather than broad or mass surveillance, which undermines fundamental rights.

International Best Practices:

India can look to international standards, such as the European Union's General Data Protection Regulation (GDPR), for guidance on balancing state security needs with the protection of privacy. Provisions for data minimization, transparency, and rights of individuals to access, correct, or delete their data should be incorporated into Indian law.

Incorporation of Technological Safeguards

Secure Data Storage and Encryption:

Data security measures must be strengthened through the use of modern encryption technologies, ensuring that personal data is securely stored and protected from unauthorized access, both by state actors and private entities.

Limiting Data Sharing: Surveillance data should only be shared between authorized entities when absolutely necessary and with proper safeguards in place to prevent abuse. A legal framework for data sharing and processing must be developed that includes clear limitations and accountability mechanisms.

Conclusion:-

While surveillance and data collection are necessary tools for maintaining national security and public order, they must not be exercised at the cost of individual freedoms and rights. Current laws governing surveillance, such as the Indian Telegraph Act and the Information Technology Act, often lack sufficient safeguards against

abuse, leading to potential violations of citizens' rights. The Digital Personal Data Protection Act, 2023, though a step forward, still contains provisions that could undermine privacy, particularly with broad exemptions for government access to data under the guise of national security. This demonstrates a misalignment with the principles of necessity, proportionality, and judicial oversight outlined in landmark judgments like K.S. Puttaswamy v. Union of India (2017).

Despite these concerns, the issue of surveillance remains critical for India's security. However, this must be balanced with stringent protections for individual privacy and freedom of expression. Judicial oversight, greater transparency, and a robust data protection framework are key to ensuring that surveillance measures do not disproportionately infringe upon citizens' rights. Clearer definitions of consent, transparent surveillance programs, and the establishment of independent oversight mechanisms can help ensure that any intrusion into privacy is justified, necessary, and proportionate.

The recommendations outlined in this study—strengthening data protection laws, ensuring judicial scrutiny, and promoting privacy awareness—are essential for addressing the gaps between the current legal frameworks and constitutional safeguards. By aligning surveillance laws with the rights guaranteed under Articles 19 and 21, India can establish a legal regime that respects privacy while addressing the legitimate concerns of national security. In conclusion, it is imperative that India rebalances its approach to surveillance and data protection in a manner that upholds constitutional values and ensures the protection of citizens' fundamental rights. The evolving legal landscape requires a continuous effort to refine and adapt the laws to new technological developments, ensuring that privacy and freedom of expression are not compromised in the name of security.

Acknowledgment
Nil.

Financial support and sponsorship
Nil.

Conflicts of Interest
The authors declare that there are no conflicts of interest regarding the publication of this paper

Reference:-

1. "Privacy and Data Protection Law in India" by Pavan Duggal
2. "The Right to Privacy: Arguing for Its Place in the Indian Constitution" by Sudhir Krishnaswamy and Others
3. "Law, Technology and Society: Exploring Data Protection, Privacy, and Surveillance" by Roger Brownsword
4. "Data Privacy Law: A Comparative Analysis of Asia-Pacific and European Regimes" by Graham Greenleaf
5. "Cyber Law and Information Technology" by Anirudh Rastogi
6. "Privacy and the Constitution: The Right to be Let Alone" by H.M. Seervai
7. "Data Protection Law: Approaches and Perspectives" by Dara Hallinan, Ronald Leenes, and Serge Gutwirth
8. "Surveillance, Privacy, and Security: Citizens' Perspectives" by Michael Friedewald and Others
9. "The Constitution of India" by P.M. Bakshi (for Articles 19 and 21 analysis)
10. "Information Technology Law and Practice" by Vakul Sharma