INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 4 AND ISSUE 3 OF 2024

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Free and Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 4 and Issue 3 of 2024 (Access Full Issue on - https://ijlr.iledu.in/volume-4-and-issue-3-of-2024/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 3 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE ROLE OF ADMINISTRATIVE LAW: GOVERNMENT SURVEILLANCE AND DATA PRIVACY

AUTHOR - D.NIROSHA, STUDENT AT THE TAMIL NADU DR. AMBEDKAR LAW UNIVERSITY, SCHOOL OF EXCELLENCE IN LAW.

BEST CITATION - D.NIROSHA, THE ROLE OF ADMINISTRATIVE LAW: GOVERNMENT SURVEILLANCE AND DATA PRIVACY, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 4 (3) OF 2024, PG. 712-717, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract:

This topic delves into the complex interplay between government surveillance and data privacy, focusing on the role of Administrative Law in managing these often conflicting interests. With governments increasingly relying on surveillance to ensure national security and public safety, there is growing concern about the impact on individual privacy rights. This concern is particularly acute in the digital age, where the scope and scale of data collection have expanded dramatically. The discussion explores how administrative law provides a legal framework to regulate surveillance activities, ensuring that they are conducted within legal boundaries while respecting fundamental privacy rights.

The study examines global data privacy frameworks, specifically the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023 (DPDPA), to highlight the challenges of balancing state interests with personal data protection. By comparing these frameworks, the research identifies commonalities and differences in how different jurisdictions address surveillance and privacy. Landmark cases, such as India's Aadhaar identity system, are analyzed to illustrate the practical tensions between state surveillance powers and individual privacy rights.

The paper argues that administrative law must evolve to address these challenges effectively. It should ensure greater transparency, accountability, and proportionality in government surveillance activities. Additionally, administrative law must adapt to global privacy developments to protect individuals' rights while enabling governments to fulfill their essential security functions. By analyzing how various legal systems handle these issues, the study aims to provide insights into the future direction of administrative law in the context of digital surveillance and data privacy.

Keywords: Government Surveillance, Data Privacy, Administrative Law

Introduction:

In the digital era , the balance between government surveillance and data privacy has become an increasing serious concern in the society . Governments around the world have turned to digital tools to ensure the national security and public safety, but these practices often raise serious concerns about the protection of individual privacy rights. Administrative law serves as a key legal framework that regulates government surveillance activities, ensuring that state powers do not infringe

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 3 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

upon citizens' rights. The rise of global data privacy regulations, such as the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023 (DPDPA), reflects a growing recognition of the need to protect personal data and limit government overreach.

The GDPR, widely regarded as a benchmark in global privacy law, provides strict guidelines on how personal data can be collected, stored, and processed, with hefty fines for non-compliance[1] . It has had a far-reaching impact, influencing privacy legislation worldwide, including India's DPDPA. The DPDPA sets forth similar standards in the Indian context, particularly addressing the concerns raised by India's Aadhaar identity system. Aadhaar, while facilitating access to essential services for millions, has sparked debates about the potential misuse of personal data and the threat of mass surveillance[2] . These matters highlight the challenges faced by administrative law in balancing the need for surveillance with the protection of privacy rights. This paper explores the evolving role of administrative law in regulating government surveillance, with a focus on how legal frameworks like GDPR and DPDPA manages these competing interests. By analyzing landmark cases such as Aadhaar and comparing international privacy frameworks, the research underscores the necessity for administrative law to evolve in ways that ensure transparency, accountability, and proportionality in government surveillance. The study further explores how these laws can safeguard individual rights while enabling governments to fulfill their security mandates in a rapidly digitizing world.

Overview of GDPR:

The General Data Protection Regulation (GDPR), was introduced by the European Union in 2018, it represents a crucial advancement in data privacy legislation. It establishes a rigorous standards for the collection, processing, and storage of personal data, emphasizing principles such as consent, transparency, and data minimization. GDPR mandates that organizations must obtain explicit consent from individuals before processing their data and restrict data collection to what is necessary for the specified purpose (Article 5) . This regulation extends beyond the EU, affecting any entity globally that processes the personal data of EU residents. Notably, GDPR imposes severe penalties for non-compliance, with fines reaching up to €20 million or 4% of global revenue, whichever is higher (Article 83) . These provisions aim to ensure high levels of accountability and transparency in data handling, thereby strengthening individual privacy rights and limiting the extent of both private and governmental surveillance. Organizations are required to obtain explicit consent from individuals before processing their personal data (Article 6), ensuring that data collected is strictly necessary for the intended purpose.Organizations must also perform Data Protection Impact Assessments (DPIAs) when engaging in high-risk data processing activities (Article 35) and appoint Data Protection Officers (DPOs) to oversee compliance(Article 37) . The GDPR's comprehensive approach has influenced global data protection standards, prompting similar legislative efforts worldwide, such as Brazil's General Data Protection Law (LGPD) and California's Consumer Privacy Act (CCPA). In 2019, the Court of Justice of the European Union

(CJEU) ruled on the scope of the "right to be forgotten" under the GDPR. The case arose when the French data protection authority, CNIL, fined Google for not globally removing search results after individuals in the EU requested their personal data be erased. Google argued that it should only have to remove links within the EU, not worldwide. The CJEU ruled in favor of Google, stating that the GDPR does not require global deletion of search results, meaning Google only needed to remove the data from EU domains. This case highlighted the limits of GDPR's extraterritorial reach while reinforcing privacy rights within the EU[3] .

Legal Framework for Data Privacy in India:

Constitutional Protections for Privacy and Surveillance in India:

India's legal framework for data privacy is undergoing substantial transformation, especially with the introduction of the Digital Personal Data Protection Act (DPDA), 2023. This landmark legislation signals a pivotal move towards stricter data privacy standards, aligning India more closely with global regulations like the General Data Protection Regulation (GDPR).

Historically, data privacy concerns in India have been managed through a patchwork of various laws, such as the Information Technology Act, 2000, and judicial interpretations like the Puttaswamy judgment, which recognized privacy as a fundamental right under Article 21 of the Constitution.

The DPDA aims to address the gaps in the current legal regime by providing clear rules on the collection, processing, storage, and sharing of personal data, thereby bringing clarity and consistency to India's data protection landscape. With a focus on data minimization, explicit consent, and stronger accountability measures, the DPDA places stringent requirements on both government bodies and private entities handling personal data. This marks a critical step forward in safeguarding individuals' privacy in an increasingly digital world, while also setting a framework that is more equipped to address the challenges posed by modern technologies.

Article 21: Right to Life and Personal Liberty
Privacy in India is constitutionally grounded in Article 21, which ensures the right to life and personal liberty. In Justice K.S. Puttaswamy (Retd) v. Union of India ,(2017), the Supreme Court recognized privacy as a fundamental right, subject to legality, necessity, and proportionality [4]. This case formed the basis for protecting personal data and limiting state surveillance within lawful limits.

Article 14: Right to Equality
Article 14 mandates equality before the law, ensuring that data protection and surveillance laws apply uniformly, without arbitrary discrimination. Surveillance measures must meet the test of fairness and cannot target specific groups without justified reasons.

Article 19(1)(a): Freedom of Speech and Expression
Article 19(1)(a) safeguards the freedom of speech, and excessive surveillance can infringe on this right by deterring free expression. The Supreme Court, in PUCL v.Union of India (1997), ruled that surveillance must be legally justified to avoid curbing free speech [5].

Article 19(1)(d): Freedom of Movement
Article 19(1)(d) guarantees freedom of movement, which could be compromised by surveillance tools like GPS tracking. Any

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 3 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

restriction on movement through surveillance must be legally justified.

Article 20(3): Protection Against Self-incrimination

Article 20(3) protects individuals from self-incrimination, extending to digital data, ensuring they cannot be forced to disclose information that may incriminate them, including passwords or biometric data.

Article 32: Right to Constitutional Remedies

Article 32 empowers citizens to seek judicial remedies when their privacy rights are violated. This provision allows individuals to challenge unconstitutional surveillance or misuse of personal data.

Statutory Frameworks Governing Data Privacy and Surveillance:

The **Information Technology (IT) Act, 2000** serves as a fundamental piece of legislation for data privacy in India. **Section 43A** mandates that companies handling sensitive personal data must implement robust security practices, holding them accountable for any negligence leading to unauthorized disclosures. Furthermore, **Section 72A** imposes penalties on individuals or entities who breach confidentiality by accessing and disclosing personal data without consent. On the surveillance side, **Section 69** of the Act grants the government the authority to intercept, monitor, and decrypt digital information in the interest of national security. However, this provision has sparked debates on potential overreach. The Shreya Singhal v. Union of India (2015)[6] case underscored the need for checks and balances, ensuring that the state's power to regulate the internet does not curtail individual freedoms .

Under Section 5(2) of the Indian Telegraph Act, 1885, the government has the power to intercept messages during public emergencies or for public safety. The Supreme Court, in PUCL v. Union of India (1997)[7], set procedural safeguards for surveillance, stating that the interception orders should be limited in duration and subject to review by a committee to prevent misuse of power PUCL v. Union of India . This precedent was further reinforced in the Anuradha Bhasin v. Union of India (2020)[8] case, where the indefinite suspension of internet services in Jammu and Kashmir was deemed a violation of the right to free speech and privacy.

The Aadhaar Act, 2016 (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) governs the use of biometric data for identity verification and access to government services. The Supreme Court, in the landmark Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) judgment, ruled that Aadhaar could not be made mandatory for services like banking and telecommunications, as this would infringe on citizens' right to privacy.The judgment emphasized the need for stronger privacy protections, particularly in light of the growing use of biometric data.

The **Unlawful Activities (Prevention) Act (UAPA), 1967** UAPA grants the government broad powers to monitor and collect data from individuals or organizations suspected of involvement in terrorist activities. In the case of Gautam Navlakha v. National Investigation Agency (2021)[9], the judiciary scrutinized the balance between national security and individual privacy, reaffirming that surveillance under the UAPA must follow legal procedures to avoid unjust infringement on civil liberties.

The National Security Act (NSA), 1980, allows preventive detention without trial in matters concerning national security, which also includes the surveillance of individuals suspected of being a threat. In A.K. Roy v. Union of India (1982)[10], the Supreme Court upheld preventive detention but stressed that procedural safeguards must be followed to prevent arbitrary surveillance and detention . The Court reiterated the need for oversight to ensure that the NSA's broad powers are not misused.

The **Personal Data Protection Bill, 2019**, aims to further regulate the use of personal data in India, drawing inspiration from the **GDPR**. The bill introduces obligations on data fiduciaries regarding data handling and processing, and outlines government surveillance provisions in the interest of national security. However, concerns have been raised over clauses that allow the government to exempt its agencies from the bill's requirements, leading to fears of unchecked state surveillance .

Conclusion :

To conclude, India's legal framework for data privacy and surveillance has made notable advancements, particularly with the recognition of privacy as a fundamental right in the landmark case of Justice K.S. Puttaswamy v. Union of India (2017) and the enactment of laws such as the Aadhaar Act, 2016 and the Information Technology Act, 2000. Despite these developments, there are still significant challenges, especially when balancing the protection of individual privacy rights and the government's need for surveillance to ensure the national security. The Digital Personal Data Protection Act, 2023 (DPDA) is a step in the right direction, bringing India's privacy regulations closer to global standards. However, the concerns remain regarding the potential for misuse of surveillance powers and insufficient oversight mechanisms.

To improve the current legal framework, several measures should be implemented. strengthening judicial oversight of surveillance activities would ensure that government agencies are held accountable, reducing the potential for abuse of power. Mechanisms similar to those outlined in PUCL v. Union of India (1997), which regulate the duration and justification for wiretapping, could be applied to digital surveillance. Additionally, the Personal Data Protection Bill should impose stricter limits on government exemptions to prevent unchecked surveillance, with transparency requirements that mandate government agencies to regularly disclose their surveillance activities.

Additionally, there should be an increased emphasis on enhancing data security practices across both the public and private sectors, such as employing stronger encryption methods and adopting data minimization principles, as seen in the GDPR. Public awareness campaigns could also be beneficial, educating individuals on their rights to privacy and how to seek redress if their data is mishandled. These measures would foster a more accountable and transparent system, ensuring that both privacy and security are adequately protected.

Reference

1. Kuner, C., Bygrave, L. A., & Docksey, C. (2019). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press.

2. Bhandari, V. (2019). "Privacy and Data Protection in India: The Need for a Data

Protection Authority." Journal of Law and Technology.

3. Google LLC v. CNIL (2019), Court of Justice of the European Union (CJEU), Case C-507/17.

4. 10 SCC 1, AIR 2017 SC 4161

5. AIR 1997 SC 568, (1997) 1 SCC 30

6. AIR 2015 SC 1523.

7. AIR 1997 SC 568.

8. 3 SCC 637, 2020 SCC OnLine SC 25, AIR 2020 SC 1308

9. AIR ONLINE 2021 SC 246

10. AIR 1982 SC 710