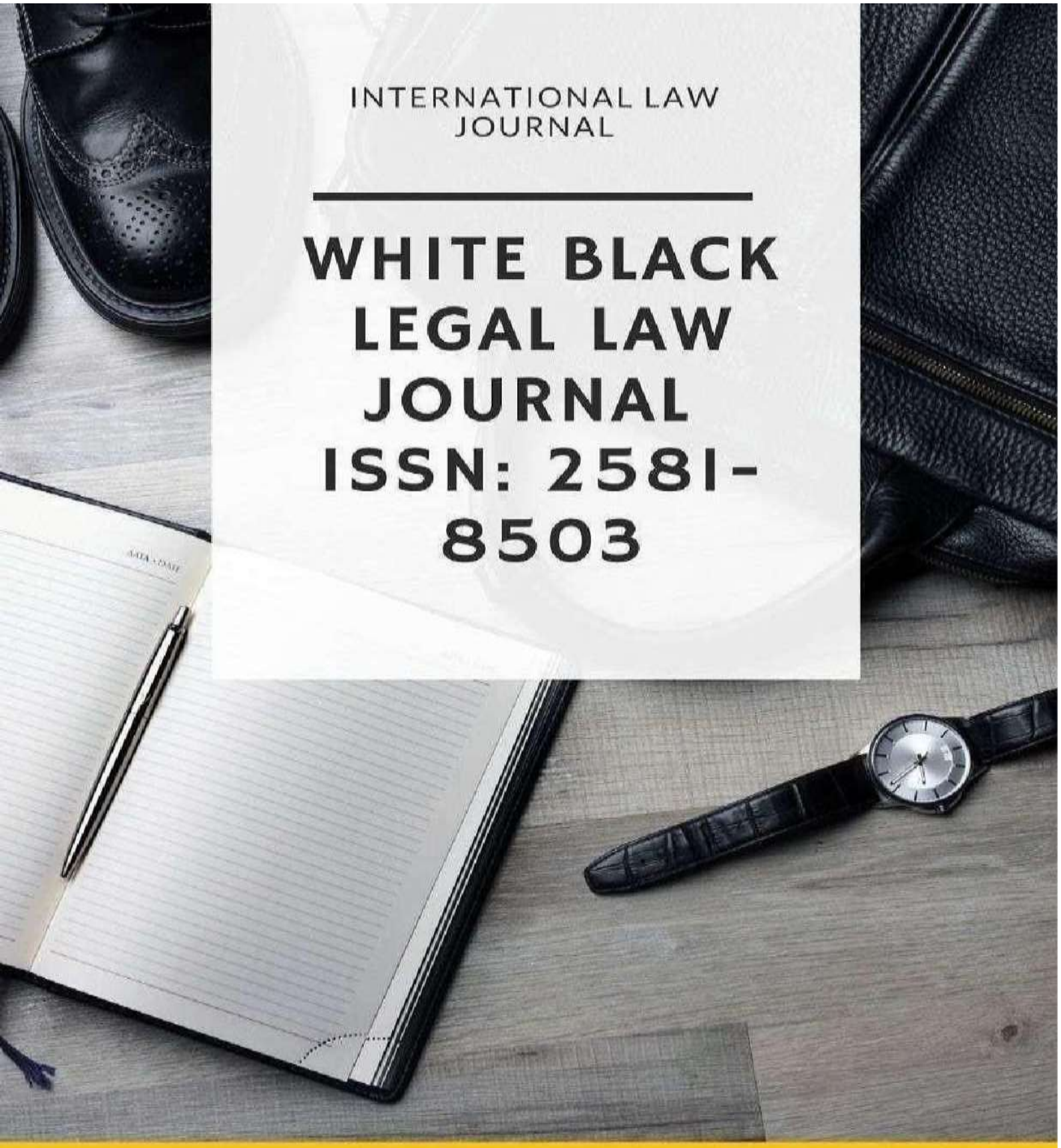

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK LEGAL

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

DATA PRIVACY AND SURVEILLANCE IN THE DIGITAL AGE: WITH SPECIAL REFERENCE TO DPDP ACT[1]

AUTHORED BY - AASHNA BANSAL

Abstract

In the age of data capitalism and digital governance, personal data has become both a valuable asset and a tool for surveillance. The increasing use of digital technologies by state and non-state actors has intensified concerns about individual privacy and the scope of data surveillance. India's response to these challenges culminated in the enactment of the Digital Personal Data Protection Act (DPDP), 2023. This paper critically examines the evolving landscape of data privacy and surveillance, analyzes the provisions of the DPDP Act, and assesses whether it adequately safeguards citizens' fundamental rights in the digital ecosystem. It also compares India's regulatory regime with international standards, identifies implementation challenges, and suggests policy improvements to balance privacy and security in a digital democracy.

Introduction

The digital revolution has fundamentally transformed the landscape of human interaction, governance, and rights. The proliferation of smartphones, internet connectivity, artificial intelligence (AI), and big data analytics has embedded digital technologies into the very fabric of modern life. In this environment, the collection, storage, and processing of personal data have become not just routine but essential components of both public administration and private enterprise. Governments collect data for welfare distribution, law enforcement, and national security, while private corporations leverage user data to drive targeted advertising, improve services, and innovate new business models.[2]

However, this datafication of society has also brought forth profound concerns regarding individual autonomy, privacy, and civil liberties. Personal data, once considered incidental, has

[1] Authored by Aashna Bansal
[2] Arun, C. (2018). Rebalancing Regulation and Rights in India's Internet Governance. Centre for Internet and Society.

now become a potent asset[3]—one that can be used not only for innovation and governance but also for profiling, discrimination, and intrusive surveillance. Particularly alarming is the manner in which surveillance technologies—such as facial recognition, biometric identification systems, and predictive policing tools—are being deployed without adequate legal safeguards or public accountability. The potential for misuse is magnified in jurisdictions with weak oversight frameworks, raising urgent questions about the balance between security and liberty.[4]

It is in this context that the Digital Personal Data Protection (DPDP) Act, 2023, emerges as a landmark legislative development in India. Enacted after years of deliberation, judicial advocacy, and civil society pressure, the DPDP Act represents India's first comprehensive attempt to establish a statutory framework for the protection of personal data. The Act defines the rights of individuals (data principals), the obligations of entities processing data (data fiduciaries), and the contours of lawful data processing. It also provides for the establishment of a Data Protection Board to oversee compliance and adjudicate disputes.

Yet, despite its promising framework, the DPDP Act has generated significant debate. While it aims to protect individual privacy in line with the Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017)[5], critics argue that the Act falls short on several counts—particularly with regard to state surveillance and government exemptions. The law permits the central government to exempt its agencies from compliance, raising concerns about unchecked executive power and erosion of judicial oversight. Moreover, the independence of the Data Protection Board is questioned, and the Act's silence on surveillance reforms has sparked apprehension among rights advocates and legal scholars.

This research explores the complex interplay between data privacy and state surveillance in the digital age, with a special focus on the efficacy and implications of the DPDP Act, 2023. It seeks to critically assess the extent to which the Act addresses the dual imperatives of safeguarding personal data and enabling lawful state surveillance. The central questions guiding this inquiry are: How does the DPDP Act strike a balance between data protection and national security imperatives? Does it adequately protect individual privacy in light of

[3] Choudhury, M. (2023). *Data Protection Law in India: Business First, Rights Later*. Software Freedom Law Center India.
[4] Bhatia, G. (2019). *The Transformative Constitution: A Radical Biography in Nine Acts*. HarperCollins India
[5] Justice K.S. Puttaswamy v. Union of India (2017)

constitutional guarantees and international human rights norms? Additionally, the study will evaluate how the Act compares with global data protection frameworks such as the EU's General Data Protection Regulation (GDPR) and Brazil's Lei Geral de Proteção de Dados (LGPD), and whether it reflects a rights-based approach grounded in democratic accountability.

In doing so, the research contributes to the broader discourse on digital rights, state power, and constitutionalism in the 21st century. It argues that while the DPDP Act is a step forward, a truly effective data protection regime must be rooted in principles of transparency, proportionality, judicial scrutiny, and the separation of powers. As India aspires to be a global digital leader, the challenge lies in ensuring that its data governance model upholds the sanctity of individual rights while addressing legitimate state concerns—a balance that will shape the contours of Indian democracy in the digital era.

Literature Review

The discourse on data privacy and surveillance has garnered considerable scholarly attention over the past two decades, especially in light of growing digitization, algorithmic governance, and expansive state surveillance. This literature review critically engages with key theoretical frameworks, legal analyses, and comparative studies that shape the current understanding of data protection in India and globally. It also highlights gaps that the present study seeks to address, particularly with reference to the Digital Personal Data Protection (DPDP) Act, 2023.[6]

1. Theoretical Foundations of Privacy

Scholars such as **Alan Westin (1967)** have classically defined privacy as "the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated." This liberal, individual-rights-based understanding forms the cornerstone of privacy jurisprudence in democratic societies. **Daniel Solove (2008)** expands this notion by proposing a taxonomy of privacy, categorizing threats as surveillance, aggregation, insecurity, secondary use, and exclusion. These theoretical lenses continue to inform judicial reasoning and legislative drafting worldwide.[7]

[6] Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer.
[7] Greenleaf, G. (2023). *India's DPDP Bill 2023: GDPR-Lite or Business-Friendly Privacy?* Privacy Laws & Business International Report, (183), 1–6.

2. Surveillance and the State

A growing body of literature critiques the normalization of state surveillance in the name of national security. **David Lyon (2003)** characterizes modern surveillance as part of the "surveillance society," where data collection by the state and corporations becomes systemic and often opaque. In the Indian context, **Usha Ramanathan (2017)** critically examines the Aadhaar project as a techno-legal infrastructure that enables mass surveillance without sufficient legal accountability. Similarly, **Anja Kovacs** and the **Internet Democracy Project** argue that digital surveillance in India operates in a legal vacuum, often bypassing principles of due process.

3. Constitutional Developments and Judicial Perspectives

The landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017) is widely regarded as a constitutional turning point. **Gautam Bhatia (2019)**, in *The Transformative Constitution*, argues that the ruling reorients Indian constitutionalism towards individual autonomy and dignity, providing a foundational basis for data protection legislation. **Chinmayi Arun (2018)** cautions, however, that while the judgment lays out broad principles, operationalizing these into enforceable statutory protections requires institutional will and legislative precision—both of which remain lacking.[8]

4. Comparative Legal Studies

Comparative studies have often benchmarked India's data protection efforts against the European Union's **General Data Protection Regulation (GDPR)**. **Greenleaf (2023)** notes that while India's DPDP Act borrows terminologies such as "data fiduciary" and "data principal," it diverges significantly from the GDPR in terms of oversight, rights enforcement, and limitation on state access. **Gonzalez Fuster (2014)** underscores the GDPR's emphasis on independent supervisory authorities, transparency, and data minimization—elements not fully reflected in India's framework.

5. Surveillance Law in India

Legal scholars have long critiqued the lack of comprehensive surveillance laws in India. **Srinivas Kodali (2021)** and the **Internet Freedom Foundation** argue that laws such as the Indian Telegraph Act (1885) and the IT Act (2000) are outdated and inadequate to deal with

[8] *Justice K.S. Puttaswamy v. Union of India* (2017)

contemporary digital surveillance practices. There is a persistent demand for a legal architecture that includes judicial oversight, necessity-proportionality tests, and parliamentary accountability—demands that the DPDP Act does not meet.

6. Critiques of the DPDP Act, 2023

Initial analyses of the DPDP Act, 2023, such as those by **Mozilla Foundation (2023)** and **Internet Freedom Foundation (2023)**, have pointed out several areas of concern. These include:

- The overbroad exemptions granted to government agencies (Section 17),
- The lack of independence of the Data Protection Board,
- Opaque consent mechanisms,
- And the dilution of earlier safeguards proposed in draft versions.

Mishi Choudhary (2023) critiques the Act as being more aligned with facilitating ease of doing business than upholding fundamental rights. Her work highlights the need for embedding the law within a constitutional rights framework rather than treating it merely as a compliance regime.

7. Gaps in Existing Literature

While there is considerable scholarship on privacy theory and critiques of surveillance, there remains a lacuna in:

- **Empirical evaluations** of how citizens perceive and exercise their data rights,
- **Detailed analysis** of the interplay between the DPDP Act and India's surveillance architecture,
- And **jurisprudential integration** of the DPDP Act within the framework of the *Puttaswamy* decision and global rights-based benchmarks.

This research seeks to bridge these gaps by critically analyzing the DPDP Act through a constitutional and comparative lens, with a focus on the tension between state surveillance and individual rights.

Research Questions

This study is guided by the following key research questions:

1. **How does the DPDP Act, 2023, address the challenges of data privacy in India's digital environment?**

2. **To what extent does the DPDP Act provide safeguards against mass surveillance and unauthorized data access by state agencies?**
3. **How does the Indian data protection regime compare with international frameworks such as the GDPR and Brazil's LGPD in terms of rights protection and regulatory oversight?**
4. **What are the structural, legal, and practical limitations of the DPDP Act in ensuring robust data privacy and democratic accountability?**
5. **What reforms are needed to create a balanced approach between privacy protection and national security in the Indian context?**

Methodology

This research adopts a **doctrinal legal research methodology**, complemented by **comparative and analytical approaches**. The methods used are as follows:

- **Primary Sources**: Analysis of statutes (e.g., DPDP Act, 2023; IT Act, 2000; Indian Constitution), case law (notably *Justice K.S. Puttaswamy v. Union of India*), and parliamentary documents.
- **Secondary Sources**: Review of academic journals, policy briefs, think-tank reports, and expert commentary.
- **Comparative Analysis**: Evaluation of data privacy and surveillance regimes in other jurisdictions (e.g., GDPR in the EU, LGPD in Brazil) to draw lessons and benchmarks.
- **Doctrinal Review**: Examination of legal principles, interpretations, and rights-based discourse emerging from court decisions and constitutional norms.
- **Normative Assessment**: The research also incorporates a critical rights-based lens to assess whether the DPDP Act aligns with democratic and constitutional ideals.

This qualitative methodology aims to provide a nuanced, legally sound, and contextually grounded understanding of privacy and surveillance in the digital age.

Scope and Limitations

Scope:

- The paper focuses on **Indian data privacy and surveillance laws**, especially the **DPDP Act, 2023**, within the constitutional and global comparative framework.
- It includes references to **international standards** and comparisons with other privacy regimes to evaluate the relative adequacy of India's approach.

- Both **state** and **corporate** data practices are considered, with emphasis on **state surveillance**.

Limitations:

- The research is largely **legal-analytical** and does not include empirical fieldwork or surveys.
- The DPDP Act is newly enacted, and **judicial interpretation and practical implementation** are still evolving.
- While comparisons are made, full exploration of **non-legal technological aspects** (like encryption or AI-driven surveillance tools) is outside the scope.

Evolution of Data Privacy Norms

Global Legal Framework

Globally, data privacy has emerged as a critical human rights issue. The European Union's General Data Protection Regulation (GDPR), enacted in 2018, set a benchmark for comprehensive data protection laws. It is built on principles like consent, purpose limitation, data minimization, and accountability. Other countries, including Canada, the UK, and Australia, have adopted similar frameworks, integrating privacy into their legal and policy regimes.

India's Constitutional Backdrop

In India, the right to privacy was elevated to a fundamental right under **Article 21** by the Supreme Court in **Justice K.S. Puttaswamy v. Union of India (2017)**. The judgment recognized privacy as intrinsic to life and liberty, laying the foundation for future data protection legislation. The court also acknowledged the need for a robust legal framework to regulate data collection, storage, and usage.

Legislative Trajectory Pre-DPDP

Prior to the DPDP Act, India's data protection regime was fragmented. The **Information Technology Act, 2000** and its accompanying rules (especially the SPDI Rules, 2011) were the primary instruments governing data privacy. However, these lacked comprehensiveness and enforceability, prompting the formation of various expert committees and multiple draft bills, culminating in the DPDP Act, 2023.

Surveillance in the Digital Era

The Rise of Digital Surveillance

Surveillance technologies—ranging from facial recognition and biometric tracking to spyware like Pegasus—have significantly expanded state capacity for monitoring citizens. While surveillance can aid in national security and crime prevention, it often lacks legal accountability in India. Multiple agencies operate without clear legislative mandates or judicial oversight.

Legal Gaps and Oversight Issues

India lacks a dedicated surveillance law. Agencies like the Intelligence Bureau (IB) and Research and Analysis Wing (RAW) function based on executive orders rather than statutory legislation. The **Indian Telegraph Act, 1885** and **Information Technology Act, 2000** are used to authorize surveillance, but both are outdated and inadequate for the complexities of digital data flows.

Chilling Effect and Civil Liberties

Unchecked surveillance leads to a 'chilling effect' on speech and expression, as citizens fear being monitored. This violates democratic norms and contradicts India's constitutional vision. The lack of judicial oversight and absence of data minimization standards further exacerbate the issue.

The Digital Personal Data Protection (DPDP) Act, 2023: A Critical Analysis

Key Features of the DPDP Act

The DPDP Act, 2023, aims to establish a comprehensive framework for personal data protection. Key provisions include:

- **Scope and Applicability**: Applies to digital personal data processed in India and abroad if related to Indian data principals.
- **Consent-Based Processing**: Personal data processing requires valid, informed consent.
- **Rights of Data Principals**: Includes right to information, correction, erasure, grievance redressal, and consent withdrawal.
- **Obligations of Data Fiduciaries**: Entities processing data must implement security safeguards, report breaches, and ensure compliance.
- **Exemptions for State**: Allows government agencies to be exempted in matters of national security, sovereignty, and public order.

- **Establishment of Data Protection Board**: To enforce compliance and adjudicate violations.

Strengths of the Act

- **Codifies Privacy Rights**: Gives statutory recognition to key privacy principles.
- **Introduces Accountability**: Sets obligations for data fiduciaries and establishes penalties.
- **Digital-First Design**: Recognizes the realities of a tech-driven society.

Criticism and Limitations

1. **Excessive Government Exemptions**: Section 17 empowers the central government to exempt agencies from any or all provisions of the Act, undermining the privacy framework.
2. **Lack of Independence**: The Data Protection Board lacks autonomy, as its members are appointed by the government.
3. **Absence of Data Localization Mandates**: Unlike earlier drafts, the final version does not require local storage of sensitive data.
4. **No Safeguards for Surveillance Reform**: The Act fails to regulate state surveillance mechanisms or incorporate judicial oversight.

Comparative Perspectives

India vs. EU (GDPR)

The GDPR offers stronger protection through its **principle-based approach** and **independent supervisory authorities**. It also has **strict limitations on surveillance**, requiring that state access to data be "necessary and proportionate."

India vs. USA

The U.S. lacks a unified data protection law but has sector-specific laws (e.g., HIPAA, COPPA). However, U.S. surveillance mechanisms under laws like the **PATRIOT Act** have faced criticism for overreach, much like India's own systems.

India vs. Brazil (LGPD)

Brazil's **LGPD** closely mirrors the GDPR and ensures **independent oversight**, **transparency**, and **public consultations**—elements missing from India's DPDP regime.

Challenges in Implementation

1. **Institutional Capacity**: Effective enforcement requires trained personnel, digital infrastructure, and inter-agency coordination.
2. **Public Awareness**: A large portion of India's population lacks digital literacy, limiting the practical exercise of privacy rights.
3. **Corporate Compliance**: Ensuring data fiduciaries, especially start-ups and SMEs, comply with the law without undue burden is a delicate task.
4. **Surveillance Accountability**: The absence of a law regulating intelligence agencies leaves a gaping hole in the privacy architecture.

Recommendations

1. **Amend Section 17**: Narrow the scope of exemptions to ensure they are necessary, proportionate, and subject to judicial review.
2. **Strengthen Oversight Mechanisms**: Make the Data Protection Board independent, with transparent appointment processes and parliamentary oversight.
3. **Surveillance Law Reform**: Enact a dedicated law for surveillance, ensuring legality, necessity, proportionality, and due process.
4. **Enhance Public Awareness**: Launch nationwide campaigns to educate citizens about their data rights.
5. **Cross-Border Data Governance**: Negotiate bilateral and multilateral data transfer agreements to align with global standards.

Conclusion

The Digital Personal Data Protection (DPDP) Act, 2023, represents a significant milestone in India's journey toward establishing a comprehensive and modern legal framework for digital governance and personal data protection. It is the culmination of years of deliberation, expert recommendations, public consultations, and judicial advocacy emphasizing the need for a rights-based approach to data privacy. By codifying the rights of data principals and delineating the responsibilities of data fiduciaries, the Act lays the groundwork for a data governance regime aligned with the needs of a rapidly digitizing society. However, despite these commendable strides, the Act's transformative potential is undermined by several critical shortcomings.

Foremost among these is the provision allowing the central government to exempt its agencies from the Act's obligations on broad and vaguely defined grounds such as sovereignty, public order, and national security. These sweeping exemptions create a parallel regime where state surveillance and data processing activities can occur without meaningful oversight, transparency, or accountability. This not only weakens the privacy rights of individuals but also risks institutionalizing unchecked executive power. Furthermore, the structural design of the Data Protection Board, the regulatory body envisioned under the Act, lacks the independence and autonomy necessary for impartial enforcement. Its composition, appointment process, and operational control remain tethered to executive discretion, raising concerns about regulatory capture and the dilution of citizens' rights.

Compounding these issues is the Act's silence on reforming India's existing surveillance architecture, which continues to operate in legal grey zones without robust judicial or parliamentary scrutiny. In the absence of an overarching surveillance law, agencies can exploit legal ambiguities to conduct mass surveillance, often without consent or procedural safeguards. This contradicts the principles laid down by the Supreme Court in the *Puttaswamy* judgment, which emphasized legality, necessity, and proportionality as prerequisites for any state intrusion into privacy.

In a constitutional democracy governed by the rule of law, it is imperative that the state is not the sole arbiter of what constitutes reasonable limitations on privacy. Independent oversight mechanisms, judicial review, and legislative accountability are essential to ensure that data protection laws do not become tools of authoritarianism. A truly robust data protection regime must strike a careful balance between the imperatives of national security and the fundamental rights of individuals. Such a balance can only be achieved through a rights-centric approach that emphasizes transparency, proportionality, due process, and public trust.

As India positions itself as a global leader in the digital economy and technological innovation, it must simultaneously commit to protecting the digital rights of its citizens. Privacy is not merely a legal entitlement but a cornerstone of individual autonomy and democratic expression. Upholding the sanctity of this right in the digital age is not only a constitutional obligation but a democratic imperative that will shape the ethical foundation of India's digital future.