INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

BALANCING PRIVACY AND STATE SURVEILLANCE: A COMPARTIVE ANALYSIS OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT WITH GLOBAL DATA PROTECTION REGIMES

AUTHORED BY - DRISHTI PANDEY

ABSTRACT

The fast rise of digital governance has profoundly altered the relationship between individuals and the state, exacerbating the underlying contradiction between privacy and surveillance. In India, this transition is constitutionally anchored by Justice K.S. Puttaswamy v. Union of India, which elevated privacy to the status of a fundamental right. However, the legislative reaction, particularly the Digital Personal Data Protection Act of 2023 (DPDP Act), is part of a larger ecosystem of surveillance regulations that give the state enormous powers.

This study conducts a detailed and comparative review of India's data protection framework, taking into account recent developments such as the DPDP Rules for 2025[1], ongoing constitutional challenges, and surveillance controversies such as the Pegasus spyware litigation. The study contends that India's framework remains structurally uneven by comparing it to worldwide standards, particularly the European Union's GDPR and jurisprudence such as Schrems II (2020). While it uses the language of data protection, it also legitimizes broad surveillance. The report concludes that genuine reform necessitates rebalancing the system through judicial monitoring, institutional independence, and stronger proportionality norms.

KEYWORDS

Privacy; Surveillance; DPDP Act 2023; DPDP Rules 2025; Pegasus; Informational Privacy; Constitutional Law; Data Governance; Proportionality.

[1] Digital Personal Data Protection Rules,2025

1. INTRODUCTION

"Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet." – Gary

India, which has a crime rate of 445.9 per 1,000,000 inhabitants and is the second most targeted country by hackers, frequently faces security risks from both internal and external sources, including borderless terrorism. Numerous rules that regulate communications and information exchange in the digital realm are used to solve these issues. Furthermore, some important areas of concern that often go unnoticed by such restrictions are unauthorized trade, theft, and misuse of personal data.

In Europe, instances of such unapproved transfers have been reported, and possible government abuse has been noted. The General Data Protection Regulation was implemented as a way to safeguard personal information. The recent introduction of the Personal Data Protection regime in India has sparked a debate about it that demands a critical examination of its rules, which are drafted with a similar goal in mind.

The development of digital technology has made personal data an essential tool for governance. In order to provide welfare benefits, control economic activity, and maintain national security, states are depending more and more on data-driven technologies. But the same technologies that make effective governance possible also make it possible for previously unheard-of levels of surveillance, which puts conventional ideas of privacy and individual liberty at jeopardy.

India's legal response to this transformation has been shaped by constitutional jurisprudence and legislative intervention. The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India [2](2017) marked a decisive shift, establishing privacy as intrinsic to human dignity and liberty. This doctrinal foundation led to the enactment of the DPDP Act, 2023, which seeks to regulate the processing of digital personal data.

Yet, the Indian legal framework governing surveillance extends beyond this Act. Colonial-era statutes such as the Telegraph Act, 1885, and modern legislation like the Information

[2] K.S. Puttaswamy v. Union of India,AIR 2017SC4161

Technology Act, 2000 continue to authorize extensive state surveillance. Recent developments including the operationalization of the DPDP Rules, 2025 and controversies surrounding spyware have further intensified the debate on privacy[3].

2. CONCEPTUAL FRAMEWORK: PRIVACY, SURVELLIANCE AND PROPORTIONALITY

According to contemporary constitutional law, privacy is a multifaceted right that encompasses decision-making freedom, informational autonomy, and bodily integrity. It is essential to the functioning of a democratic society and provides protection against arbitrary state intrusion.

Conversely, national security is the defense of the state against dangers to its integrity, sovereignty, and public order. Potential dangers include organized crime, cyberattacks, terrorism, and espionage. The state employs surveillance as a preventive and investigative tool to address such risks. Monitoring communications, collecting information, and tracking potentially dangerous activities are all part of surveillance. Although surveillance can strengthen national security, it also poses serious privacy and civil liberties issues. Maintaining public confidence in governmental institutions while guaranteeing citizens' safety requires striking a balance between these concerns. If these privacy issues are not resolved, community relations may suffer and people may become less trusting of law enforcement. Therefore, it is crucial that legislators create precise rules that uphold people's rights while allowing for efficient surveillance techniques.The fundamental goal of surveillance is to protect society as a whole. However, surveillance can go beyond justifiable security requirements and invade the personal lives of regular people if it is widespread, ongoing, or poorly regulated. In contrast, surveillance is an example of the use of sovereign power. Unchecked surveillance seriously jeopardizes civil liberties, even though it may be justified for reasons like public order or national security.

According to recent research, surveillance not only violates privacy but also has a "chilling effect[4]," deterring people from using their basic rights.

[3] https://assets.kpmg.com/content/dam/kpmgsites/in.PDF/2025/11/dpdp-rules-2025-guidance-to-dpdp-act-implementation.pdf

[4] https://journals.safe pub.com/Do I/10.1177/20539517211065368

The main method for striking a balance between these conflicting interests is the proportionality doctrine. It stipulates that any limitations on rights must be justified by the law, have a justifiable purpose, be necessary, and strike a balance between the means and the goal.

3. CONSTITUTIONAL FRAMEWORK OF PRIVACY IN INDIA

Early development of privacy rights can be observed from **Kharak Singh v. State of U.P[5].** where the Supreme Court of India addressed privacy in the context of police surveillance. The court ruled that the right to privacy was implied in the right to personal liberty under Article 21, but it did not get explicitly recognized as a fundamental right.

The scope of the privacy rights expanded in the case of **R. Rajagopal v. State of Tamil Nadu[6]** where the Supreme Court recognized the right to privacy as an aspect of Article 21. In this case the publication of a person's life story was involved without consent, leading to a broader interpretation of privacy.

Justice K.S. Puttaswamy v. Union of India (2017)- The Supreme Court's decision in *Puttaswamy* represents a paradigm shift in Indian constitutional law. The Court recognized privacy as an inherent part of the right to life and personal liberty, emphasizing its role in protecting dignity, autonomy, and freedom.The judgment established a structured proportionality test and highlighted the need for safeguards against state surveillance.Most importantly, it acknowledged the risks posed by digital technologies, thereby laying the groundwork for future data protection legislation.

People's Union for Civil Liberties v. Union of India[7] - In this case, the Supreme Court addressed the legality of telephone tapping under the Telegraph Act. While upholding the State's power to intercept communications, the Court introduced procedural safeguards to prevent arbitrary use.

However, these safeguards were designed for a pre-digital era and are inadequate in addressing modern surveillance technologies.

[5] Kharak Singh v. State of U.P.,AIR 1963 SC 1295
[6] R. Rajagopal v. State of Tamil Nadu, AIR 1994 SCC(6) 632
[7] **People's Union for Civil Liberties v. Union of India, AIR 1997 SC 568**

Anuradha Bhasin v. Union of India[8]- The Court extended privacy protections into the digital domain by emphasizing that restrictions on internet access must satisfy the test of proportionality. In this case underscored the importance of digital rights in contemporary constitutional law.

4. LEGISLATIVE DEVELOPMENTS IN INDIA AND CURRENT SCENARIO

In the digital age, privacy protection in India is a dynamic and multifaceted issue[9]. While various legislative and regulatory frameworks exist, a significant advancement was made with the enactment of the India Digital Personal Data Protection Act 2023 (DPDPA). This landmark legislation, effective from September 1, 2023, aims to safeguard individuals' privacy in the digital realm by imposing rigorous privacy and data protection standards on all organizations processing personal data in India. The following outlines the current landscape of privacy protection legislation in India.

1. Information Technology Act, 2000 (IT Act)

- Sections 43A and 72A: These sections deal with compensation for failure to protect data and punishment for breach of confidentiality and privacy, respectively.
- IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: These rules define what constitutes sensitive personal data and outline the security practices companies must follow to protect such data.
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: This rule mandates that companies collecting information must adhere to specific requirements to ensure the security of private data.

2. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act,

- Section 29: Restricts the sharing of core biometric information.

[8] Anuradha Bhasin v. Union of India, AIR 2020 SC 1308
[9] https://Legal ons.com/case-analysis-of-k-s-puttaswamy-vs-union-of-india-2017-landmark-judgememt-on -right-to-privavy

- Section 30: Classifies biometric information as sensitive personal data.
- Section 33: Allows disclosure of information in the interest of national security upon direction by an officer not below the rank of Joint Secretary.

3. Right to Information Act, 2005 (RTI Act)

- Section 8(1)(j): Exempts personal information from disclosure if it has no relationship to any public activity or interest, or if it would cause an unwarranted invasion of privacy unless the larger public interest justifies the disclosure.

4. The Bharatiya Nyaya Sanhita, 2023

- Sections 314 and 316(1): Address dishonest misappropriation of property and breach of trust, which can relate to misuse of personal information.

5. Consumer Protection Act, 2019

- Consumer Protection (E-Commerce) Rules, 2020: Includes provisions related to the protection of consumer data in e-commerce transactions.

6. Telecom Regulatory Authority of India (TRAI) Regulations

- Telecom Commercial Communications Customer Preference Regulations, 2018: Aims to curb unsolicited commercial communication and protect user data in the telecom sector.

7. Sector-Specific Guidelines

- Reserve Bank of India (RBI) Guidelines: The RBI issues guidelines for banks and financial institutions regarding data protection and cybersecurity.
- National Health Data Management Policy, 2020: Provides guidelines for the protection of health data.

8. The Digital Personal Data Protection Act, 2023

The DPDPA safeguards personal data processed within India, irrespective of its origin. Additionally, the Act extends its protection to the personal data of Indian citizens, even if the

processing occurs outside India

Emerging Surveillance Technologies

Technological advancements have significantly expanded the scope of surveillance. Systems such as CMS and NATGRID enable large-scale data collection and integration, raising concerns about mass surveillance.

The Pegasus spyware controversy exemplifies these concerns. Reports indicate that spyware has been used globally, including against individuals in India, raising serious constitutional questions about unauthorized surveillance and privacy violations.

The Supreme Court, while examining the issue, acknowledged that surveillance must be consistent with constitutional guarantees and cannot be justified solely on grounds of national security.

5. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND RECENT DEVELOPMENTS

India's first comprehensive data protection law is the DPDP Act[10]. It creates a framework based on accountability, purpose limitation, and consent.

5.1 DPDP Regulations, 2025

The Act became operational in November 2025 with the release of the DPDP Rules, which offered useful implementation guidelines.

These regulations impose obligations on data fiduciaries, improve user rights, and establish compliance mechanisms. By focusing on transparency and data minimization, they also hope to bring India's framework into compliance with international norms.

[10] https://www.hoganlovells.com/en/publication/indias-digital-personal-data-protection-act-2023-brought-into-force

Critics counter that the Rules still prioritize state interests over individual rights, which exacerbates worries about surveillance.

Stakeholders are advocating for a more balanced strategy that protects individual privacy while simultaneously attending to national security requirements as the discussion surrounding these regulations progresses. In order to guarantee that the interests of both individuals and society are sufficiently represented, the changing data protection landscape in India will necessitate constant discussion.

5.2 Constitutional Objections to the DPDP Act

Some of the DPDP Act's provisions, especially those that give the State broad exemptions, have been challenged as unconstitutional in recent Supreme Court petitions.

These difficulties call into question the Act's compatibility with Articles 14, 19, and 21[11], especially with regard to accountability and transparency.

5.3 Legal Action for Pegasus Surveillance

In the discussion of surveillance, the Pegasus controversy has taken center stage. Acknowledging the stifling impact such actions have on freedom of expression, the Supreme Court established an expert committee to look into claims of unlawful surveillance.

The case demonstrates how inadequate current legal frameworks are when it comes to dealing with cutting-edge surveillance technologies.

5.4 New Policy Issues

Recent proposals, like making smartphone location tracking mandatory, have drawn harsh criticism from international organizations and civil society, who caution that such actions could result in widespread surveillance.

[11] The Constitution of India

Concerns about how data protection laws affect press freedom have also been voiced, and stakeholders have emphasized the need for more precise protections.

6. GDPR AND DPDP ACT OVERVIEW

Since May 2018, the European Union has been enforcing the General Data Protection Regulation[12] (GDPR). It is regarded as the world's most extensive data protection legislation. It governed how controllers and processors, both inside and outside the EU, handled personal data. It is founded on the ideas of accountability, transparency, and fairness. Individuals are given a wide range of rights, including profitability, erasure, correction, access, and processing objection. Any breaches must be reported by the organization within 72 hours. GDPR is a global standard for privacy governance because it is enforced by independent supervisory authorities and carries fines of up to 20 euro million, or 4% of global annual turnover.

7. SCOPE AND APPLICATION OF GDPR AND DPDP

The GDPR has a broader application as it covers both digital personal data and data stored in physical form. This in contrast to DPDP is different as the proposed bill only covers personal data collected online and in digitized form. Additionally both legislations apply to processing of personal data within and outside the country or union subject to processing happening for data subjects present in the member states or for purpose of offering activities within the territory. For instance, DPDP applies to processing of personal data outside its territory only when the activities involve profiling i.e. predicting or analysing behaviour of the data subject. Similarly, where the controller or processor is not established within the union, but the behaviour of data subjects is monitored within the union provisions of GDPR will apply.

This ensures that individuals' rights are protected regardless of where their data is processed.

Consequently, organizations must remain vigilant in adhering to these regulations to avoid potential penalties and maintain trust with their users.

Therefore, the only thing that needs to be noted is whether or not the processing is done to monitor behavior or provide services within the union or nation. It is important to remember that

[12] https://www.trade.gov/market-intelligence/eu-general-data-protection-regulation-gdpr

processing involves more than just communicating and transferring personal information; it also involves storing and loading that information onto a website or web page. Therefore, before decoding the scope and ambit of the proposed bill and GDPR, it is important to understand the purpose for which the personal data is being processed. However, there are situations in which the proposed bill and GDPR do not apply. One of these circumstances is when personal information is processed for domestic or personal purposes.

Other situations in which GDPR and DPDP do not apply include those in which personal data is "processed for preventing, investigating, and prosecuting any violation in law." However, in the case of GDPR, such processing of personal data is governed by Directive (EU) 2016/680 in the EU and is subject to specific union law. Conversely, the proposed bill makes no mention of this.

8. COMPARATIVE INTERNATIONAL JURISPRUDENCE

Comparative analysis shows that while international regimes place more emphasis on individual rights and institutional accountability, India's strategy is still state-centric. India's framework differs from international best practices due to its lack of independent oversight mechanisms and extensive statutory exemptions. The best way to assess the advantages and disadvantages of India's privacy framework is to compare it to other data protection laws or regimes. In contrast, the US, UK, EU, and other BRIC nations offer the standard and model for assessing the framework. The regimes' variations in various contexts and domains, such as "regulatory scope, constitutional bases, and mechanisms for enforcement," are the reason for the thorough comparison.

8.1 The European Union

GDPR was passed by the EU in 2018 and has since become the standard for data protection worldwide. According to "The Charter of Fundamental Rights of the European Union's Article 8," data protection is regarded by this act as a fundamental human right[13]. Therefore, regardless of the location of the establishment, the GDPR applies extraterritorially to any entity that

[13] https://gdpr-info.EU/recitals/no-1

processes the personal data of EU citizens or residents. As a result, the GDPR's definition of "personal" data is more expansive, but enhanced data protection focuses on ethnic, biometric, and health data as "special categories." Additionally, the framework calls for informed consent that is "freely given, specified, informed, and unambiguous." Individuals have consequently been granted a wide range of rights, such as "portability, erasure, rectification, access, and automated decision-making objection." In order to guarantee that member states have consistently applied the law, the European Data Protection Board (EDPB) coordinates the supervisory authorities.

Administrative fines can reach €20 million. Strict restrictions have also been placed on cross-border data transfers, which are only allowed in states with "adequate" protections or "under standard contractual clauses."

Cases like Big Brother Watch v. United Kingdom[14] and Klass v. Germany[15]demonstrate that surveillance needs to be supported by strong protections.

8.2 The United Kingdom

Following Brexit, the GDPR was preserved through the Data Protection Act of 2018, which led to the creation of "the UK GDPR." With rights like "access, erasure, rectification, restriction of processing and portability," this largely mirrored the EU model. The Information Commissioner's Officer (ICO), who oversees independent regulation, has the authority to impose fines of up to £17.5 for infractions. However, the UK government recently proposed significant reforms, with "data protection simplification" being the driving force behind these initiatives, despite experts' concerns about protection dilution. Despite the recent developments, the UK GDPR is primarily a rights-based regime that is in line with the EU model.

8.3 The United States

State-specific and patchwork sectorial statutes are used instead of a single, comprehensive federal data protection law in the United States. The Fourth Amendment provides limited protection for privacy, primarily aimed at preventing government surveillance. However, certain areas are protected by sector-specific laws such as the Health Insurance Portability and

[14] Big Brother Watch v. United Kingdom, 2021
[15] Klass v. Germany, 1978

Accountability Act (HIPAA) and the Children Online Privacy Protection Act (COPPA). The most important state-level data protection law is the California Consumer Privacy Act (CCPA). With broad consumer rights to "deletion, access, and opt-out of data sale," the California Privacy Rights Act (CPRA) was recently passed. Together with state attorneys general, the California Privacy Protection Act (CPPA) serves as the enforcement body. However, rather than employing a universal rights-based approach, this model is primarily fragmented and prioritizes consumer protection. As a result, opt-out consent mechanisms are promoted instead of opt-in, and there is little consistency across sectors or states.

The Court acknowledged the sensitivity of digital data and placed restrictions on surveillance in Carpenter v. United States[16].

8.4 BRICS

One of the BRICS countries, Brazil, has regulatory protections through its "Lei general de Protecao de Dados (LGPD)," which clearly follows the same GDPR principles. While China relies on "Personal Information Protection (PIPL)," South Africa is guided in safeguarding these rights by the "Protection of Personal Information (POPIA)." However, China and Russia stand out due to their emphasis on "sovereignty and state surveillance." These nations make sure that strict safeguards are in place at the local level, but state authority is generally increasing the accessibility of personal data. All things considered, the BRICS countries share a commitment to data governance, despite notable variations in how state interests and individual rights are balanced.

9. CRITICAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

There is a structural imbalance between privacy and surveillance in the Indian legal system. Although the protection of privacy is emphasized in constitutional jurisprudence, these principles are frequently compromised by statutory laws and executive actions. The coexistence of strong

[16] Carpenter v. United States, 585 U.S. 296 (2018)

constitutional guarantees and weak statutory safeguards creates a normative contradiction, limiting the practical realization of privacy rights.An important turning point in the defense of individual privacy in the digital age is the India Digital Personal Data Protection Act 2023 (DPDPA). This comprehensive legislation will take effect on September 1, 2023, and it will apply to all organizations that process personal data of Indian citizens both domestically and internationally. The DPDPA's main goal is to protect individual privacy by enforcing strict data protection regulations on businesses.

According to the DPDPA, any information that can directly or indirectly identify a natural person is considered personal data. Names, addresses, contact details, dates of birth, gender, financial information like credit card numbers and bank account numbers, online browsing history, social media activity, and location data like GPS coordinates are all included in this broad definition. The DPDPA guarantees complete protection of personal data by covering such a wide range of information.

Regardless of its source, personal data processed in India is protected by the DPDPA, which also extends its protection to Indian citizens' personal data processed abroad. However, some categories of data are not covered by the Act, such as information used for personal or family use, journalism or artistic expression, and law enforcement or national security. The Data Protection Authority of India (DPA), an independent organization in charge of guaranteeing adherence to the Act, is in charge of enforcing the DPDPA. The DPA has the power to look into complaints, impose penalties, and require businesses to follow the set data protection guidelines. The DPA plays a vital role in protecting people's right to privacy through these measures.

To sum up, the India Digital Personal Data Protection Act 2023 is an all-encompassing attempt to safeguard personal privacy in the digital age. The DPDPA seeks to establish a safe and open environment for processing personal data by defining personal data broadly, establishing important data protection principles, and giving individuals substantial rights. The Act, which is upheld by the Data Protection Authority of India, guarantees that businesses adhere to these guidelines, improving the general security and privacy of personal data in India.

10. FUTURE DIRECTIONS AND THE CASE FOR GLOBAL HARMONISATION

10.1 IN THE DIRECTION OF CONVERGING DATA PROTECTION STANDARDS

The disparate nature of data protection laws presents significant challenges for cross-border governance, business compliance, and the protection of fundamental rights as digital technologies expand and operate on a global scale. When India, the EU, and the US are compared, there is a noticeable lack of coherence in their legislative frameworks, enforcement strategies, and underlying ideologies. This discrepancy highlights the increasing need for international data protection standards to converge and harmonize.

The emergence of the EU's GDPR as a global standard is one encouraging development. Japan, South Korea, Brazil, and South Africa are among the nations that have either signed adequacy agreements with the EU or passed laws inspired by the GDPR. In order to guarantee worldwide compliance, even businesses situated in countries with laxer regulations, like the US, are increasingly coordinating their internal data governance frameworks with the GDPR. 292 The global discourse on privacy has been significantly shaped by the "Brussels Effect," in which EU regulatory standards impact international standards because of market power and extraterritorial applicability. Partially in line with the GDPR, India's Digital Personal Data Protection Act, 2023 places a strong emphasis on user consent, purpose limitation, and accountability. But in important areas like algorithmic transparency, government access restrictions, and the lack of a robust, independent regulatory body, the legislation falls short. India needs to align with international best practices and bolster procedural safeguards in order to achieve true convergence, especially as it looks to expand its digital economy and form international data partnerships.

There is growing pressure in the US to enact a comprehensive federal privacy law. The growing number of state-level laws, like the California Consumer Privacy Act (CCPA), has resulted in a disjointed legal system that is unfair and ineffective. In addition to streamlining business compliance, a federal framework based on GDPR principles—such as data minimization, accountability, and data subject rights—could better safeguard American citizens in the digital era.

Preemption and private right of action discussions, however, continue to be major roadblocks to congressional consensus. Lastly, the long-term viability of any data protection policy will depend on public awareness, digital literacy, and civil society involvement. In all three jurisdictions, privacy must move beyond elite legal discourse and become part of the broader public consciousness. Education, advocacy, and access to redress mechanisms must be made universally available to empower individuals to assert their rights in a complex and data-driven world.

10.2 Opportunities for Global Collaboration and Innovation in Regulation

The role of multilateral organizations like the Organization for Economic Co-operation and Development (OECD), United Nations (UN), and G20, which have the capacity to establish soft law frameworks or model regulations for data governance, must be taken into consideration in efforts toward global harmonization. The OECD Privacy Guidelines, which were first published in 1980 and revised in 2013, are still used as a guide for national laws that uphold the values of security, justice, and individual involvement. However, these rules are voluntary and have no legal force behind them.

The idea of "Data Free Flow with Trust" (DFFT), which aims to strike a balance between robust data protection measures and economic growth, was first presented in the G20 Osaka Leaders' Declaration (2019). DFFT offers a forum for communication and collaboration between nations with disparate legal systems and values, despite still being in its early stages. Participation in G20 discussions by the US, EU, and India presents a strategic chance to create common frameworks for cross-border data flows.

11. CONCLUSION

India's data protection laws are at a turning point. Even though the DPDP Act and recent advancements are noteworthy, they are insufficient to address the more fundamental structural problems with the surveillance system. Both are necessary for a democratic state to function and need to be carefully balanced. India's constitutional framework offers a solid basis for this balance, especially after privacy was acknowledged as a fundamental right. Court rulings have made it clear that any invasion of privacy must be justified, essential, and reasonable. However, with little

independent oversight and transparency, the current legal framework governing surveillance still mainly depends on executive discretion. Although data protection laws are a step forward, their protective effect is diminished by widespread exemptions for state agencies, particularly when it comes to surveillance. The analysis shows that how surveillance should be regulated, rather than whether it should exist, is the main concern. Unchecked surveillance runs the risk of undermining democratic values by discouraging free speech and eroding public institution trust. Comprehensive reforms, such as judicial oversight, institutional independence, and increased transparency, are necessary to achieve a meaningful balance between privacy and surveillance.