International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

Organised Crime under the Bharatiya Nyaya Sanhita, 2023: A Critical Evaluation of Scope and Safeguards

Dr. Cheshta Dahiya
Assistant Professor at Vivekananda, Institute of Professional Studies, (TC), New Delhi

Abstract
The rapid growth of India's digital economy has brought unprecedented opportunities as well as challenges in ensuring the privacy and protection of personal data. This paper aims to critically analyze India's current data protection framework, focusing on the provisions of the Personal Data Protection Bill, 2019 (PDPB), and evaluating its effectiveness in safeguarding citizens' privacy. In order to provide a comprehensive understanding, the PDPB is compared with global standards, including the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA). The study employs a mixed-methods approach combining comparative legal analysis and survey data collected from 300 respondents across urban, semi-urban, and rural regions. The survey investigates public awareness of data privacy regulations, their concerns regarding personal data security, and preferences for data handling practices. Key findings indicate that while India has made significant strides through the PDPB, substantial gaps remain in terms of enforcement, transparency, and alignment with internationally recognized data protection norms. The paper argues that harmonizing India's legal framework with global standards is essential to ensure robust consumer protection, build public trust in the digital ecosystem, and facilitate secure technological innovation.

Keywords: Data Protection, Privacy Law, Personal Data Protection Bill, 2019, GDPR, CCPA, Legal Reform, India

1. Introduction

India's digital economy has been experiencing rapid growth over the past decade, fueled by increasing internet penetration, the proliferation of digital services, and the adoption of emerging technologies such as artificial intelligence, e-commerce platforms, and cloud computing. This expansion has created significant opportunities for economic development and innovation, but it has also amplified concerns regarding the privacy and security of personal data. With millions of citizens engaging online daily, safeguarding sensitive information has become a critical priority. Despite this digital advancement, India's existing legal framework for data protection remains inadequate. The Information Technology Act, 2000, which primarily governs data security and cyber offences, was enacted at a time when digital services were in their infancy. Consequently, it lacks comprehensive provisions to address modern challenges such as large-scale data breaches, cross-border data flows, and the complexities of data processing by both private and government entities. The absence of

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

detailed mechanisms for consumer rights, enforcement, and accountability has created a regulatory gap, leaving individuals vulnerable to misuse of their personal information.

Recognizing these deficiencies, the Personal Data Protection Bill, 2019 (PDPB) was introduced with the objective of establishing a robust legal framework to protect personal data in India. However, questions remain regarding its effectiveness, clarity, and alignment with global data protection standards such as the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA).

Research Problem

India's current data protection laws are insufficient to address the evolving landscape of digital privacy. This study seeks to examine how effectively the PDPB safeguards citizens' personal data and identify the areas where it may fall short compared to international standards.

Objectives

1. To analyze India's current data protection framework, focusing on the provisions of the PDPB, 2019.
2. To compare the PDPB with global standards, including GDPR and CCPA, highlighting similarities, differences, and gaps.
3. To evaluate the practical implications of the PDPB for consumers and suggest areas for legal reform and improvement.

2. Literature Review

2.1 Privacy as a Fundamental Right

The right to privacy has been increasingly recognized as a cornerstone of individual liberty and autonomy in the digital age. In India, the landmark Justice K.S. Puttaswamy v. Union of India (2017) case established privacy as a fundamental right under Article 21 of the Constitution, laying the foundation for subsequent data protection laws. Privacy is no longer limited to physical spaces but extends to personal information, digital transactions, and communication. As the collection and processing of personal data have grown exponentially, safeguarding privacy has become critical to ensuring both individual rights and public trust in digital services.

2.2 Key Academic Contributions

Several scholars have examined India's data protection framework and its limitations:

- **Batra (2020)** critiques India's existing data protection regime, highlighting the inadequacies of the Information Technology Act, 2000, and emphasizing the need for comprehensive legislation to protect citizens from modern cyber risks.
- **Verma (2019)** analyzes the provisions of the Personal Data Protection Bill, 2019, identifying its strengths, such as data localization and consent mechanisms, as well as weaknesses, including weak enforcement provisions and limited clarity on government access to personal data.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

- **Kumar & Singh (2021)** focus on the challenges in implementing the PDPB, emphasizing the lack of clear mechanisms for consumer rights protection and the need for capacity building within regulatory authorities to ensure compliance and accountability.

These studies collectively highlight the significance of legal reforms but also underscore the gaps in enforcement, consumer protection, and alignment with global best practices.

2.3 Global Standards Discussion

To evaluate the robustness of India's data protection framework, it is essential to compare it with international standards:

- **General Data Protection Regulation (GDPR):** Enacted by the European Union in 2018, the GDPR is widely regarded as the global benchmark for data protection. It emphasizes principles such as data minimization, purpose limitation, individual consent, the right to erasure ("right to be forgotten"), and strong enforcement mechanisms, including substantial penalties for non-compliance.
- **California Consumer Privacy Act (CCPA):** The CCPA focuses on consumer rights, providing individuals with the ability to know, delete, and opt-out of the sale of personal information. While narrower in scope than the GDPR, the CCPA has influenced data protection laws globally and represents a consumer-centric approach to privacy governance.

2.4 Research Gap

Despite extensive literature on India's PDPB and global data protection laws, there is a lack of studies that provide a comprehensive, comparative framework analyzing the alignment, gaps, and practical implications of the PDPB relative to GDPR and CCPA. Most existing research evaluates Indian and global laws separately, without offering a structured comparison that can inform legal reforms or policy recommendations. This gap underscores the need for a detailed study that combines doctrinal analysis with empirical insights, such as survey data, to assess public awareness, concerns, and preferences regarding data privacy in India.

3. Methodology

This study employs a mixed-methods approach combining qualitative legal analysis, survey research, and case study comparisons to provide a comprehensive understanding of India's data protection framework and its alignment with global standards.

3.1 Qualitative Comparative Analysis

A core component of this research is a qualitative comparative analysis of the Personal Data Protection Bill, 2019 (PDPB) with international data protection laws, namely the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA). This analysis involves examining statutory provisions, enforcement mechanisms, and consumer rights under each framework. Key focus areas include consent requirements, data subject rights, obligations of data processors, and penalties for non-compliance. The comparative method allows identification of gaps in India's legislative framework and highlights areas where the PDPB can be refined to align with globally recognized best practices.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

3.2 Survey Method

To complement the doctrinal analysis, the study incorporates empirical insights through a structured survey conducted among 300 respondents across urban, semi-urban, and rural regions in India. The survey investigates:

- Awareness of existing data privacy regulations and the PDPB, 2019.
- Levels of concern regarding personal data security and online privacy.
- Preferences for data handling, such as consent mechanisms, transparency, and data control.

The survey responses were quantified to calculate frequencies and percentages, allowing for a clear understanding of public perception, which is critical for evaluating the practical effectiveness of data protection laws.

3.3 Case Study Comparison

Additionally, a case study approach is employed to examine real-world applications and challenges in data protection. Selected case studies include notable instances of data breaches, enforcement actions under GDPR and CCPA, and Indian legal precedents related to privacy. This component provides contextual insights into how data protection provisions operate in practice, identifies enforcement challenges, and evaluates the effectiveness of safeguards provided to consumers.

3.4 Integration of Methods

By integrating doctrinal analysis, survey data, and case studies, this study achieves a holistic perspective on data protection in India. The combined methodology ensures that both the legal provisions and their practical implications are analyzed, enabling evidence-based recommendations for aligning the PDPB with international standards while addressing local challenges.

4. Survey Results

This section presents the findings from the survey conducted among 300 respondents to assess their awareness, concerns, and preferences regarding data privacy. The results are organized into tables for clarity, showing the frequency of responses in percentages for each question. These tables make it easy to interpret patterns, compare groups, and summarize public opinion on issues such as general awareness, data protection rights, and consumer preferences.

Tables provide a visual and structured representation of the survey data, making the analysis transparent and easy to understand.

Table 1: Demographic Profile

Particulars	**Frequency in Percentage**
Age	
18 to 24 Years	16.67%
25 to 34 Years	26.67%

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

35 to 44 Years	20%
45 to 54 Years	23.33%
55+ Years	13.33%
Gender	
Male	46.67%
Female	50%
Non-binary	1.67%
Prefer not to say	1.67%
Location	
Urban	60%
Semi-Urban	26.67%
Rural	13.33%

The survey captured the demographic profile of the 300 respondents to ensure a diverse representation. In terms of age, the largest group of participants was 25 to 34 years (26.67%), followed by 45 to 54 years (23.33%) and 35 to 44 years (20%), while younger respondents aged 18 to 24 years constituted 16.67% and those above 55 years 13.33%. Regarding gender, the sample was nearly balanced, with 50% female, 46.67% male, and small proportions identifying as non-binary (1.67%) or prefer not to say (1.67%). In terms of location, the majority of respondents were from urban areas (60%), while semi-urban (26.67%) and rural (13.33%) regions were also represented, providing a broad perspective across different geographic settings.

Table 2: General Data Privacy Awareness

Particulars	**Frequency in Percentage**
How aware are you of data privacy regulations (PDPB, 2019)?	
Very aware	50%
Somewhat aware	40%
Not aware at all	10%
Have you ever read a privacy policy before agreeing to it?	
Yes	66.67%

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

No	26.67%
Occasionally	6.67%
How concerned are you about the privacy of your personal data?	
Very concerned	60%
Somewhat concerned	30%
Not concerned	10%

The survey results indicate varying levels of awareness and concern regarding data privacy among respondents. Half of the participants (50%) reported being very aware of data privacy regulations such as the PDPB, 2019, while 40% were somewhat aware and 10% were not aware at all. When asked about reading privacy policies, a majority (66.67%) confirmed that they had read a privacy policy before agreeing to it, whereas 26.67% had not, and 6.67% did so occasionally. Regarding concern for personal data privacy, most respondents were highly attentive, with 60% very concerned, 30% somewhat concerned, and 10% not concerned, reflecting a generally strong awareness and caution among the public about their personal data.

Table 3: Data Protection & Consumer Rights

Particulars	**Frequency in Percentage**
Should individuals have the right to request deletion of their data?	
Yes	90%
No	5%
Unsure	5%
Would you support legislation forcing companies to disclose how your data is used?	
Strongly support	60%
Support	33.33%
Do not support	3.33%
Unsure	3.33%
Willingness to pay for data protection and security	
Yes	40%
No	50%
Maybe	10%

The survey reveals strong support among respondents for data protection rights and transparency. A vast majority (90%) believe that individuals should have the right to request deletion of their personal data, while only 5% disagreed and another 5% were unsure. When asked about legislation requiring companies to disclose how personal data is used, 60% strongly supported such measures, and 33.33% supported them, with minimal opposition

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

(3.33%) or uncertainty (3.33%). Regarding willingness to pay for enhanced data protection and security, respondents were more divided: 40% were willing to pay, 50% were not, and 10% remained undecided, indicating that while consumers value privacy, financial considerations influence their willingness to invest in additional safeguards.

Table 4: Consumer Preferences for Data Handling

Particulars	**Frequency in Percentage**
Which of the following would make you feel more comfortable sharing personal data?	
Clear privacy policies	40%
Control over data	46.67%
Opt-out options	16.67%
Data security	50%
Transparency reports	43.33%
If you were asked to provide personal data, would you prefer an easy-to-understand explanation of how your data will be used?	
Yes	83.33%
No	10%
Maybe	6.67%
How likely are you to trust a company with your personal data if they comply with global standards like GDPR?	
Very likely	66.67%
Likely	26.67%
Not likely	5%
Not at all	1.67%

The survey results highlight key factors that influence respondents' comfort and trust in sharing personal data. When asked what would make them feel more comfortable, 50% prioritized data security, followed by control over data (46.67%), transparency reports (43.33%), and clear privacy policies (40%), while 16.67% valued opt-out options. A significant majority (83.33%) indicated that they would prefer an easy-to-understand explanation of how their personal data will be used, demonstrating the importance of clarity and transparency. Regarding trust in companies that comply with global standards such as GDPR, most respondents were positive, with 66.67% very likely to trust such companies, 26.67% likely, and only a small minority

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

expressing distrust (5% not likely, 1.67% not at all), showing that adherence to international standards strongly influences consumer confidence. Example:

5. Legal Analysis

5.1 Section 1: Legal Framework

India

India's legal framework for data protection has evolved over the years to respond to the challenges posed by rapid digitization. The Information Technology Act, 2000 was the first major legislation addressing cybercrime and electronic data security. While it provides provisions against hacking, unauthorized access, and misuse of digital information, it was primarily designed for an era when online data processing was limited. The Act does not comprehensively address modern concerns such as personal data privacy, large-scale data processing, cross-border data transfers, or mechanisms for consumer consent and redress.

Recognizing these gaps, the Personal Data Protection Bill, 2019 (PDPB) was introduced to establish a robust legal framework for safeguarding personal data in India. The PDPB focuses on principles such as consent-based data processing, data localization, and rights of data subjects including access, correction, and erasure of personal information. It also proposes the creation of a Data Protection Authority to oversee compliance and enforce penalties. While the PDPB represents a significant step forward, concerns remain regarding its enforcement capacity, clarity on government access to data, and alignment with international standards.

Global Standards

In comparison, the General Data Protection Regulation (GDPR) of the European Union sets a high benchmark for data protection globally. It emphasizes individual rights such as data portability, the right to be forgotten, and stringent obligations for data controllers, with substantial penalties for non-compliance. Similarly, the California Consumer Privacy Act (CCPA) provides consumer-centric protections, enabling individuals to know, delete, and opt out of the sale of their personal information. These global standards provide a model for transparency, accountability, and strong enforcement mechanisms, highlighting areas where India's PDPB can be further strengthened.

5.2 Section 2: Case Law

The foundation of India's data protection laws is rooted in the recognition of privacy as a fundamental right. In the landmark case Justice K.S. Puttaswamy v. Union of India (2017), the Supreme Court of India held that the right to privacy is protected under Article 21 of the Constitution, which guarantees the right to life and personal liberty. This judgment has been pivotal in shaping India's approach to personal data protection, establishing the constitutional basis for legislations such as the PDPB.

The Puttaswamy case underscores that privacy encompasses control over personal information, autonomy in personal decision-making, and protection from unwarranted intrusion by the state or private entities. It provides the legal rationale for provisions in the PDPB that seek consent for data processing, rights of access and correction, and limitations on governmental access to

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

personal data. This judicial precedent has thus become the cornerstone for evaluating both the adequacy and the enforcement of data protection laws in India.

5.3 Section 3: Comparative Analysis of PDPB, GDPR, and CCPA

A comparative analysis of India's Personal Data Protection Bill, 2019 (PDPB) with global standards such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) highlights the strengths and weaknesses of each framework with respect to consumer rights, government oversight, and enforcement mechanisms. The following table summarizes key differences:

Issue	PDPB	GDPR	CCPA
Right to be forgotten	Weak	Strong	Moderate
Data portability	Limited	Strong	Limited
Government access	Broad	Strict limits	Moderate
Opt-out right	Weak	Moderate	Strong

The comparative analysis shows that while the PDPB provides basic data protection, it lags behind GDPR and CCPA in key areas. The right to be forgotten and data portability are weaker under PDPB, opt-out rights are limited, and government access is broader compared to stricter safeguards in GDPR. Overall, PDPB requires strengthening to align with global standards and ensure stronger consumer protection.

6. Critical Discussion

While the Personal Data Protection Bill, 2019 (PDPB) represents a major step forward in India's effort to safeguard personal data, several critical challenges limit its effectiveness in practice.

6.1 Weak Enforcement Mechanisms

One of the primary concerns is the limited enforcement capacity of the Data Protection Authority (DPA) envisioned under the PDPB. Although the Bill provides for penalties and compliance oversight, the regulatory framework lacks sufficient clarity on operational procedures, resource allocation, and timelines for enforcement. This raises the risk that violations may go unpunished or be inconsistently addressed, undermining public confidence in data protection measures.

6.2 Government Access Concerns

The PDPB permits broad government access to personal data for purposes including national security, law enforcement, and regulatory oversight. While some government access is necessary, the Bill does not clearly define limitations, oversight mechanisms, or transparency requirements, creating potential for misuse and erosion of privacy rights. Compared with global standards such as the GDPR, which enforces strict conditions and proportionality checks for government access, India's framework appears vulnerable to overreach.

6.3 Data Localization Problems

The Bill mandates local storage of critical personal data, which raises both operational and economic challenges. Organizations may face increased compliance costs, technical burdens,

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

and limitations on cross-border data flows, potentially hindering innovation and the growth of digital services. Without a well-defined and phased implementation plan, data localization requirements may create friction for businesses while providing only limited additional protection for citizens.

6.4 Institutional Capacity Issues

Another significant challenge is the institutional capacity of regulatory authorities. Effective monitoring, investigation, and enforcement require specialized expertise in data privacy, cybersecurity, and emerging technologies. Currently, India lacks sufficient trained personnel and infrastructure to ensure robust oversight, which could result in delayed action, inadequate protection, and inconsistent enforcement across sectors.

7. Policy Recommendations

To enhance the effectiveness of India's Personal Data Protection Bill, 2019 (PDPB) and align it with global standards, the following policy recommendations are proposed:

- **Align with GDPR Rights:** Strengthen consumer rights by incorporating comprehensive provisions for the right to be forgotten, data portability, and opt-out mechanisms, ensuring individuals have greater control over their personal data. Clear definitions and enforceable timelines should be established to empower citizens and improve compliance.
- **Strengthen the Data Protection Authority (DPA):** Enhance the operational capacity, autonomy, and resources of the DPA to enable effective monitoring, enforcement, and guidance. This includes recruiting skilled personnel in cybersecurity, legal compliance, and data governance, as well as creating robust procedures for handling complaints and breaches.
- **Clear and Stringent Penalties:** Introduce well-defined penalties and fines for non-compliance by both private entities and public authorities. Transparent enforcement mechanisms will deter violations and reinforce accountability, building public trust in data protection laws.
- **Public Awareness Campaigns:** Launch nationwide education and awareness initiatives to inform citizens about their data privacy rights, safe digital practices, and how to exercise their rights under the PDPB. Increased awareness will encourage compliance, empower consumers, and strengthen the culture of data protection in India.

SUMMARY

The Personal Data Protection Bill, 2019 (PDPB) represents a significant step forward in India's effort to safeguard personal data and establish a legal framework for privacy in the digital era. It lays the foundation for recognizing individual rights, consent-based data processing, and regulatory oversight. However, the analysis highlights that the Bill requires stronger enforcement mechanisms, clearer penalties, and enhanced institutional capacity to ensure effective compliance and protection of citizens' privacy. Furthermore, aligning the PDPB with global standards such as GDPR and CCPA is essential to address gaps in consumer rights, data portability, and restrictions on government access. Such alignment would not only strengthen individual protections but also facilitate international trust and cross-border digital transactions.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

Future research should focus on emerging challenges, including the implications of artificial intelligence, blockchain technologies, and cross-border data flows on privacy and security. Investigating these areas will help policymakers and stakeholders develop adaptive strategies to protect personal data in an increasingly complex and technology-driven environment.

REFERENCE

Batra, R. (2020). *Digital privacy in India: Addressing the gap in data protection law*. Journal of Cyber Law, 15(2), 45–68.

Bennett, C. J., & Raab, C. D. (2020). The governance of privacy: Policy instruments in global perspective (2nd ed.). MIT Press.

Bygrave, L. A. (2021). Data privacy law: An international perspective (2nd ed.). Oxford University Press.

California Consumer Privacy Act (CCPA), California Civil Code §§ 1798.100–1798.199 (2018).

General Data Protection Regulation (GDPR), EU Regulation 2016/679 (2016).

Ghosh, S., & Arora, S. (2020). Data localization in India: Law, policy and practice. *Indian Journal of Law and Technology*, 16(2), 1–25.

Government of India. (2000). *The Information Technology Act, 2000*. Ministry of Law and Justice.

Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, (169), 10–13.

Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), 222–228.

Kumar, A., & Singh, R. (2021). *India's privacy law reform: Challenges and opportunities*. International Journal of Privacy Law, 9(1), 14–32.

Kuner, C. (2020). The GDPR: Understanding the European data protection framework. *International Data Privacy Law*, 10(2), 123–130.

Puttaswamy v. Union of India, (2017) 10 SCC 1.

The California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (2018).

Verma, A. (2019). The Personal Data Protection Bill, 2019: A critical analysis. *Journal of Cyber Law & Policy*, 5(2), 112–130.

Verma, S. (2019). *A critical analysis of India's Personal Data Protection Bill*. Indian Journal of Law and Technology, 18(3), 98–112.