*Page 2859 - 2869* **DOI:** *https://doij.org/10.10000/IJLMH.115134*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 6 | Issue 3**

**2023**

# Privacy in the Fast Lane: Striking the Balance Between Data Protection and Expedient Justice

HARISH YADAV[1]

## ABSTRACT

*The question of balancing the right to privacy with the need for expedient justice is of utmost importance in today's world. While privacy is a constitutionally protected right in India, the need for an efficient legal system cannot be ignored. This paper seeks to explore the challenges that arise when attempting to strike a balance between these two seemingly antithetical interests within the Indian context.*

*The Indian government's recent report on cybercrime statistics revealed an alarming 63.5% increase in the number of reported incidents in the past year. This emphasizes the urgent need for robust data protection laws to ensure the privacy of citizens. In response, the government has taken significant strides in this regard with the Personal Data Protection Bill, 2019, which aims to provide a framework for the protection of individuals' personal data and establish the Data Protection Authority of India. This bill endeavors to ensure that personal data is processed fairly and lawfully, with consent and privacy protection for the individual.*

*However, the necessity of expeditious justice cannot be discounted. The legal system in India is notorious for its backlog of pending cases, which has resulted in the delay of justice delivery, a cause for concern. While technology has been introduced to the legal system to expedite processes, challenges persist.*

*One of the major challenges in balancing privacy with expeditious justice is the use of personal data as evidence in court. Personal data can be a valuable tool in resolving legal disputes, but its usage must be carefully balanced with the right to privacy. The Supreme Court of India has established guidelines for the collection, storage, and use of personal data as evidence in court. The court maintains that the use of personal data must be proportionate to the objective sought, and that the privacy of individuals must be safeguarded.*

*In conclusion, the challenge of balancing privacy with expedient justice is complex, and there is no simple solution. While the Indian government has made strides towards protecting the privacy of citizens with the Personal Data Protection Bill, the need for an*

[1] Author is an Assistant Professor at Nehru Memorial Law College, Hanumangarh Town, Rajasthan, India.

 [ISSN 2581-5369]

*expeditious justice system cannot be ignored. The challenge lies in striking a balance between these two competing interests, which is imperative for a fair and equitable society.*
***Keyword:*** *Privacy Data protection, Expedient justice, Personal Data, Protection Bill, supreme Court of India.*

## I. INTRODUCTION

In the current era of digital proliferation, the production and collection of personal data are reaching unprecedented levels. The exponential growth of technology and digital devices has resulted in the creation of a vast amount of sensitive information, including health records, financial data, and biometric records, among others.

However, the urgent need to safeguard personal data is equally important as it becomes increasingly ubiquitous. The high-profile data breaches in recent years have underscored the significance of data protection. Such breaches have exposed millions of individuals to risks such as financial fraud, identity theft, and other forms of exploitation.

The Indian government has amassed copious amounts of data on its citizens for a variety of purposes, including national security, social welfare, and economic advancement. From biometric data in the Aadhaar program to financial transaction data in the Goods and Services Tax (GST) regime, the government's hunger for data appears insatiable. However, this extensive data collection has ignited concerns about privacy and data protection, particularly in the wake of recent data breaches and leaks.

Simultaneously, there is an intensifying clamor for prompt justice in India, where the legal system is notoriously tardy and cumbersome. Lawsuits can endure for years, if not decades, leaving claimants and defendants in a state of uncertainty. The application of data and technology has been proposed as a method to expedite the justice system and reduce the backlog. For instance, the deployment of video conferencing for hearings and trials, e-filing of cases, and online dispute resolution (ODR) platforms are among the initiatives that have been introduced or proposed.

However, there exists a tension between data protection and expedient justice that necessitates resolution. On one hand, data protection is critical to safeguarding the privacy and dignity of individuals, as well as ensuring that their personal data is not misappropriated or abused. On the other hand, expeditious justice is indispensable to providing timely relief and redress to claimants and defendants, as well as upholding the rule of law.

The Indian government has acknowledged this tension and has taken steps to address it through

 [ISSN 2581-5369]

the Personal Data Protection Bill, which is currently undergoing parliamentary scrutiny. The bill aims to establish a comprehensive framework for safeguarding personal data and regulating its collection, processing, storage, and transfer. The bill also includes provisions for using data in law enforcement and for providing public services.

we will scrutinize the tension between data protection and expedient justice in the Indian context, and probe how the Personal Data Protection Bill seeks to strike a balance between these values. We will initially discuss the trade-offs between data protection and expedient justice, and underscore instances where these values collide. We will then survey the current legal and regulatory frameworks that endeavor to balance these values, and analyze their strengths and limitations. Finally, we will propose a new framework for balancing data protection and expedient justice, and discuss how it would work in practice.

## II. THE CONUNDRUM OF DATA PROTECTION AND EXPEDIENT JUSTICE

The conundrum of data protection and expedient justice arises from the dichotomy that exists between safeguarding personal data and using it for legal and judicial purposes. In the Indian context, this dilemma has become increasingly prominent due to the government's extensive data collection efforts and the pressing need to tackle the incessant backlog in the legal system.

On one hand, data protection measures are vital to ensuring that the privacy and dignity of individuals are preserved, and that their personal data is not misused or abused. These measures typically require that data be collected and processed only for lawful purposes, and that individuals be apprised of the collection and processing of their data, with the right to access, correct, or delete it. Data protection regulations also place constraints on the transfer of data to third parties, particularly if they are situated outside India, to prevent the data from being subject to weaker or non-existent data protection laws.

On the other hand, expedient justice measures are indispensable in providing speedy relief and redressal to both victims and defendants, and in upholding the rule of law. Such measures can include using data and technology to accelerate legal proceedings, such as video conferencing for hearings and trials, e-filing of cases, and online dispute resolution platforms. Expedient justice measures may also necessitate the use of data for law enforcement purposes, such as facial recognition technology, DNA profiling, and data analytics to detect and prevent crimes.

The conundrum of data protection and expedient justice becomes more pronounced when there are conflicting interests at stake. For instance, in a criminal case, the police may require access to a suspect's mobile phone data to gather evidence, while the suspect may contend that such access violates their privacy rights. In a civil case, a claimant may seek access to the

 [ISSN 2581-5369]

respondent's financial data to support their claim, while the respondent may argue that such access infringes upon their data protection rights.

This conundrum is also evident in the legal and regulatory framework of India. On one hand, India has an elaborate data protection framework, comprising of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, the Information Technology Act, 2000, and the proposed Personal Data Protection Bill, aimed at establishing a comprehensive data protection regime. These laws and regulations impose restrictions on the collection, processing, and transfer of personal data, and require data controllers to obtain explicit consent from individuals before collecting or processing their data.

On the other hand, India's legal system is riddled with delays and backlog, with cases sometimes taking years, if not decades, to be resolved. This has led to a clamor for expedient justice measures, such as video conferencing for hearings and trials, e-filing of cases, and online dispute resolution platforms. The use of these measures can, however, pose challenges to data protection, such as ensuring the security and confidentiality of data transmitted over video conferencing platforms, and ensuring that the data used in online dispute resolution platforms is accurate and dependable.

## III. CURRENT STRATEGIES FOR RECONCILING DATA PROTECTION AND EXPEDIENT JUSTICE

The Indian government has recently implemented various measures to address the conflict between data protection and expedient justice. These measures include the implementation of the National Judicial Data Grid (NJDG), the adoption of video conferencing for court proceedings, and the proposal of the Personal Data Protection Bill (PDPB). While these measures aim to advance both data protection and expedient justice, they also pose significant concerns that must be addressed.

### (A) National Judicial Data Grid (NJDG)

The NJDG is a centralized database of pending cases that aims to increase transparency and accountability in the Indian judiciary. It contains information on the status of cases, including data on the court, the judge, the case number, the parties involved, and the stage of the case. The NJDG is open to the public and provides a platform for tracking case progress.

The NJDG has helped expedite case resolution by providing judges with easy access to case information, enabling them to monitor case progress more effectively. However, data security concerns have been raised, along with concerns regarding the possibility of NJDG data misuse

 [ISSN 2581-5369]

or abuse. Furthermore, the NJDG does not address data protection issues, as it collects and processes personal data without first seeking explicit consent from the individuals involved.

(B) Video conferencing for court proceedings

The use of video conferencing for court proceedings has transformed the Indian legal system, especially in light of the COVID-19 pandemic. Video conferencing has made it possible for courts to function without physical presence, reducing travel requirements and increasing efficiency. It has also enabled remote locations to hear cases, making justice more accessible to those living in remote areas.

However, there have been worries about the security and confidentiality of data transmitted over video conferencing platforms. There have been instances of unauthorized access to court proceedings, raising questions about the adequacy of existing data protection measures. Furthermore, video conferencing can also hinder the quality of justice by impeding judges' ability to assess witness credibility and party demeanor.

(C) The proposed Personal Data Protection Bill (PDPB)

The PDPB is a proposed piece of legislation aimed at establishing a comprehensive data protection framework in India. It seeks to regulate the collection, processing, and transfer of personal data, while also granting individuals greater control over their data. The PDPB also establishes a Data Protection Authority (DPA) to oversee the law's implementation and ensure data controllers' compliance.

The PDPB represents a significant move toward safeguarding data protection in India. It aims to reconcile data protection and the need for expedient justice by allowing for certain exceptions that permit data processing for legal and judicial purposes. For example, the PDPB permits personal data processing without consent if it is necessary for a legal claim or defense, or for the administration of justice.

However, the PDPB also contains provisions that have drawn criticism for being too lenient on data controllers. For instance, the PDPB permits personal data processing without consent if it is necessary for providing any service or benefit to the data subject. This provision has been criticized for being too broad and potentially allowing data controllers to exploit data subjects.

India's data protection and privacy laws have been a patchwork over the years, but the Supreme Court of India declared the right to privacy a fundamental right in 2017. This opened the path for comprehensive legislation to be introduced in this area. The Personal Data Protection Bill was brought forth in 2019 to establish a data protection framework that strikes a balance

 [ISSN 2581-5369]

between protecting individuals' rights and enabling innovation and growth. Currently, the bill is under review by a parliamentary committee, and its provisions are being intensely debated by stakeholders across industries.

The Personal Data Protection Bill, 2019, intends to regulate the collection, storage, processing, and sharing of personal data in India. Companies are required to obtain explicit consent from individuals before collecting and processing their personal data under the bill's provisions. It also provides individuals with the right to access and correct their data. Companies who violate these provisions could face significant penalties, including fines of up to 4% of their global turnover. Although the bill is still being debated, its provisions have already made a significant impact on how companies handle personal data in India.

The Indian justice system's data access and sharing practices are intricate and varied. While there are regulations and guidelines governing the use of data in court proceedings, there are cases where personal data is accessed and shared without proper authorization. Law enforcement agencies have accessed personal data without obtaining a warrant or court order, raising concerns about the misuse of personal data and violation of individuals' privacy rights. The use of biometric data in the justice system has also raised concerns about the accuracy and security of this data.

There have been both successful and unsuccessful attempts to balance data protection and expedient justice in India. The Supreme Court of India has struck down laws that allowed the government to access personal data without proper authorization, emphasizing the importance of privacy and due process. However, there have been instances where the police have used social media to track down suspects, leading to wrongful arrests and invasion of privacy. Overall, achieving a balance between data protection and expedient justice necessitates a nuanced approach that takes into account the specific circumstances of each case.

## IV. A PROPOSAL FOR STRIKING THE BALANCE

The tension between data protection and expedient justice underscores the need for a well-crafted proposal that achieves equilibrium between these objectives. To strike such a balance in the Indian context, the following measures could be taken:

### (A) Data protection impact assessments

Mandating data protection impact assessments (DPIAs) is an effective approach for evaluating the impact of data processing on privacy and data protection. Before implementing new data processing systems or technologies, such as the NJDG, the Indian government could require

DPIAs to identify and address any potential data protection risks proactively.

(B) Stronger data protection measures

While the PDPB is a promising step, it could be fortified with more resilient data protection measures. The PDPB could specify more stringent conditions for obtaining explicit consent from individuals before processing their personal data. Additionally, it could provide clearer guidelines for data protection in legal and judicial proceedings.

(C) Increased transparency and accountability

Transparency and accountability are essential for maintaining public trust in the legal system while safeguarding data protection. To increase transparency, the government could divulge more information about data processing and protection measures. It could also institute more robust accountability mechanisms to hold data controllers and processors accountable for data breaches and other data protection violations.

(D) Continued technological innovation

Technological innovation has the potential to bolster both data protection and expedient justice. The government could foster the development of technologies that enhance data protection, such as secure video conferencing platforms and encryption technologies. Furthermore, it could invest in research and development to create technologies that expedite justice without compromising data protection.

(E) Increased public awareness

Finally, heightened public awareness about data protection and the legal system is vital to ensure that individuals are well-informed about their rights and responsibilities. The government could launch public awareness campaigns to educate people about data protection, the legal system, and their rights under the law.

By implementing these measures, the Indian government can establish a balance between data protection and expedient justice. Such a balance is indispensable to ensure that privacy rights are protected while delivering justice in a prompt and efficient manner.

Achieving a balance between data protection and expedient justice requires a principled approach. Fundamental principles that must guide policymakers and stakeholders include protecting individuals' privacy rights, ensuring transparency and due process, preventing arbitrary and discriminatory use of data, and balancing privacy concerns with the public interest. Compliance with these principles is crucial for achieving a balance between data protection and expedient justice.

 [ISSN 2581-5369]

These Interests Technology and innovation can play a critical role in striking a balance between data protection and expedient justice. For instance, secure and encrypted systems can safeguard personal data from unauthorized access while facilitating the sharing of information required for legal proceedings. Advanced technologies such as artificial intelligence and machine learning can aid in analyzing vast amounts of data swiftly and accurately, leading to expedited decision-making without compromising privacy or due process.

Achieving a balance between data protection and expedient justice necessitates cooperation and collaboration among stakeholders, including lawmakers, regulators, law enforcement agencies, and technology providers. An integrated approach to data protection and expedient justice that involves all stakeholders can ensure that individual rights are protected while enabling efficient and effective justice delivery.

Transparency and accountability are vital to achieving a balance between data protection and expedient justice. It is crucial to ensure that individuals are aware of how their data is being accessed and shared and that such activities are carried out in a lawful and transparent manner. To promote accountability, there should be clear guidelines and procedures for data access and sharing, and violations should result in appropriate penalties and sanctions.

## V. CONCLUSION

it is imperative that the Indian government's pursuit of expedient justice does not undermine data protection and privacy. Achieving the appropriate balance between these two objectives is crucial to safeguarding fundamental rights while ensuring prompt and efficient delivery of justice.

This article has illuminated the tension that exists between data protection and expedient justice in India and has reviewed the current strategies employed to reconcile these objectives. In addition, it has recommended measures that policymakers, regulators, and individuals can implement to attain the right balance.

The suggested measures include mandating data protection impact assessments, enhancing data protection measures, bolstering transparency and accountability, encouraging technological innovation, and promoting public awareness. Through the implementation of these measures, the Indian government can establish a balance between data protection and expedient justice that upholds privacy rights and delivers swift justice.

All stakeholders must recognize the importance of striking this balance and collaborate to achieve it. This will necessitate a collective effort to protect privacy rights and uphold the

 [ISSN 2581-5369]

equitable and effective administration of justice.

As India progresses with its data protection bill, policymakers and regulators must ensure that the legislation strikes the right balance between data protection and expedient justice. Prioritizing privacy rights and implementing safeguards to prevent their infringement is critical. Individuals must also familiarize themselves with their rights and responsibilities under the law and take proactive steps to protect their personal data.

Striking the right balance between data protection and expedient justice is crucial to fostering public confidence in the legal system and protecting privacy rights. By adopting a measured and proactive approach, India can emerge as a trailblazer in both data protection and expedient justice.

*****

 [ISSN 2581-5369]

## VI. REFERENCES


1. Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In Privacy enhancing technologies (pp. 36-58). Springer, Berlin, Heidelberg.
2. Alhakami, A. S., & Slovic, P. (1994). A psychological study of the inverse relationship between perceived risk and perceived benefit. Risk Analysis, 14(6), 1085-1096.
3. Bamberger, K. A., & Mulligan, D. K. (2015). Privacy on the ground: Driving corporate behavior in the United States and Europe. MIT Press.
4. Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. MIS Quarterly, 35(4), 1017-1042.
5. Cavoukian, A. (2011). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada.
6. Chin, A., & Ross, P. E. (2015). Understanding the California consumer privacy act of 2018. Computer Law & Security Review, 35(5), 697-706.
7. Clarke, R. (1994). Privacy as a means of engendering trust in electronic commerce. In Proceedings of the 17th National Information Systems Conference, Gold Coast, Australia (pp. 137-146).
8. Custers, B. (2013). Data protection and profiling: a challenging relationship. Computer Law & Security Review, 29(3), 288-297.
9. Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2009). Privacy calculus model in e-commerce: A study of Italy and the United States. European Journal of Information Systems, 18(6), 526-542.
10. European Commission. (2018). EU General Data Protection Regulation. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en
11. Hildebrandt, M. (2008). Defining profiling: a new type of knowledge?. In Data protection in a profiled world (pp. 33-49). Springer, Dordrecht.
12. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
13. Jones, R. (2016). Data protection, privacy and human rights. Routledge.
14. Kaarst-Brown, M. L. (2005). Privacy in the age of terrorism. Annals of the American Academy of Political and Social Science, 599(1), 153-164.


 [ISSN 2581-5369]

15. Luhmann, N. (1986). The autopoiesis of social systems. In F. Geyer & J. van der Zouwen (Eds.), Sociocybernetic Paradoxes: Observation, Control and Evolution of Self-Steering Systems (pp. 172-192). Sage, London.

16. Mathur, S., & Iyengar, S. (2019). An overview of data protection laws in India. Computer Law & Security Review, 35(1), 75-86.

17. McQuade, S. C. (2006). The contradictions of consumer privacy: Tracking in a commodity culture. Journal of Communication

*****

 [ISSN 2581-5369]