

Balancing Innovation and Individual Rights : A Critical Appraisal of Online Privacy and Data Protection in India

Deepak kumar¹
Dr. Amit Verma²

Abstract

The digital revolution has intensified debates surrounding online privacy and data protection, particularly in emerging economies like India, where technological innovation coexists with fragile regulatory mechanisms. This paper offers a critical appraisal of India's evolving legal and institutional framework for data protection against the backdrop of its socio-economic realities and digital ambitions. With the exponential growth of digital services, big data analytics, and AI-driven surveillance systems, concerns about individual privacy have become more urgent. The study critically examines the proposed and existing legal instruments, including the Information Technology Act and global influences like the GDPR, to highlight their conceptual, procedural, and enforcement limitations. Drawing from international comparisons, judicial precedents, and policy analyses, the paper argues that India's data protection regime must move beyond symbolic legalism to adopt a rights-based, transparent, and technologically adaptive framework. It advocates for stronger oversight mechanisms, citizen awareness programs, and privacy-enhancing technologies to balance the imperatives of individual rights and economic development.

Keywords: Data Protection, Online Privacy, Innovation, Surveillance, Indian Law.

Introduction

There has recently been a surge of interest in data protection and privacy rights issues involving the collection, storage, and use of vast quantities of personal information across the globe, primarily spurred by a significant rise in internet usage, proliferation of digital devices, and rapid growth of the information/knowledge economy worldwide, particularly in developing and emerging economies like India. Primarily because of the social, economic, and political power that result from technology, big data, the internet, and social media, after Saudi Arabia, China, Pakistan, the UAE, and Iran, the massive upsurge in the digital economy and associated political debate on right to information and individual privacy, which emboldened the civil-liberal age in many parts of the world, particularly in North America and Europe, has brought India into the limelight. In recent years, some civil society groups and judicial courts, particularly the Supreme Court, have taken a keen interest in internet privacy issues, particularly in the context of Aadhaar, a biometric and demographic database project initiated in 2009 to bring all Indian citizens under the aegis of a "unique identity" number and consequent biometric attendance in government offices and differential direct benefit transfers, which led to directives and public interest litigation owing to large scale data breaches and abuse, security concerns, and exclusion due to the unavailability of biometric "identifications."

Historical Context of Data Protection in India

The right to privacy has been accorded great significance by several countries in the world as it forms an essential component of individual liberty. The legitimacy of state interference with the fundamental rights of an individual is postulated on the principles of democracy, rule of law and constitutionalism. With a burgeoning tech-savvy populace and disruptive technology-driven start-ups, India has been hailed as the next hub of digital economy innovation.

¹ Research Scholar, Teerthanker Mahaveer University, Moradabad.

² Associate Professor, Teerthanker Mahaveer University, Moradabad.

However, the unmitigated use of individual data by tech-intermediaries has drawn the ire of scholars, academics, media, and policy-makers alike. The issue of data protection is therefore one of great national importance (Basu, 2012). The approach has been to study the legislative developments, responses of other stakeholders, regarding data protection in India, and the objectives, limitations and extent of these legislative initiatives. Individual legislations and its limited application are now juxtaposed against the need for a comprehensive omni-bus legislation covering a common understanding of data, its processing by whom and its accountability.

Key Legislation Governing Data Privacy

The journey of Data Privacy Legislation in India

This part deals primarily with the analysis of the laws that govern the data protection and privacy issues in India and an attempt to understand how the country has evolved over the time on this aspect. The Information Technology Act, 2000, which aimed at e-commerce legislation in India, was created to replace the Intermediary Liability Rules, which do not acknowledge essential rights such as data protection and privacy within the law of India. Eventually, it is observed that in India, there is a legal void until now with reference to data protection, which affects individuals; in the present scenario also, one can refrain from approaching the Indian courts as there is no legislative framework to approach the judiciary as the area is unregulated. The researcher, therefore, attempts to discuss the comparison of legislation governing cyber privacy, with reference to the recent influential legislations in the United States of America (Sood, 2015).

Existing legislation in India

1. The IT Act, 2000: the commencement of e-commerce in India
2. The IT (Amendment) Bill, 2006: adding provision, protection and privacy of personal data
3. The Draft National Data Protection Bill 2011: protection and privacy of sensitive data
4. The Draft Data Protection Bill 2013 and 2018: recommendation and consultation with the stakeholders

Existing legislation in the United States

1. Fair Information Practice Principles (FIPPs): Employee privacy
2. Federal Privacy statute: Privacy legislation for financial services-related consumer information

Accountability Mechanisms for Businesses

In order to address data protection for individuals, the GDPR mandates a future proof, high standard of accountability to all data controllers. In a rapidly developing technological ecosystem, compliance with obligations is a key challenge that needs to be met. The WP29 views accountability from the perspective of the data protection officer in organisations and as a mere paper exercise, instead of a complex socio-technical job that needs to be done. An important part of the challenge of DP compliance by design is background work that incurs a wide range of artefacts. The background work does not stop at DP compliance by design, but is ongoing and evolves throughout the life cycle of an IoT product. Therefore, the WP29's understanding of accountability fails to see the importance of context, the granularity of accountability, and how to do accountability in practice (Crabtree et al., 2018). The GDPR mandates two kinds of accountability, viz. internal and external accountability. Internal accountability aims at controlling the responsible parties, whilst external accountability aims at disciplinary mechanisms that aim at governing behavioural compliance. In the practice of IoT development, accountability as control and assurance is often more or less obligatory internal development mechanisms, such as processes, procedures, documentation and monitoring measures to keep track of compliance as part of DP by design and default. Many of these mechanisms echo the existing requirements for data protection impact rankings. An important part of external accountability mechanisms for businesses include third-party audits and certifications, some of which are well established and some not yet developed, that assure DP compliance and operations. In order to address the wide range of control and assurance mechanisms needed to do accountability in practice, we developed a taxonomy of accountability mechanisms for businesses. To derive this taxonomy, we analysed how regulation translates into monitoring compliance. Here, the focus is on how external accountability mechanisms can be used to rank compliance regarding the access to and circulation of personal information (Urquhart et al., 2018).

Public Awareness and Individual Rights

Public awareness of online privacy rights is an essential requirement for the neutrality, fairness, and competence of any privacy legislation. Many published surveys and studies provide statistical evidence of the general population's privacy experiences, opinions, and emotions. Overall awareness is minimal in India, regarding both online

privacy rights and related data protection regulations. Responses are largely uninhibited due to ignorance of existing rights, as dramatic emotional responses may not get triggered for lack of knowledge (Sood, 2015)..

Understanding Data Rights

Data rights refer to a conceptual framework that treats data as an extension of existing human rights of individuals such as privacy, autonomy, and the free expression of ideas. In particular, data rights encompass individuals' rights to manage, control, and engage with their data. Data rights were first introduced as a response to growing concerns regarding behavioral and targeted advertising practices and their effects on privacy and public perception of online platforms. However, data rights can be more broadly interpreted to include rights to receive compensation for consumer generated data, or even the right to obtain a copy of data stored by an organization. Data rights are a specific and emerging category of rights akin to existing human rights.

Given that the concept of data rights is novel and in active development, an examination of the current practices and standards with respect to data rights is opportune. Relative to data rights ideals, what is their current state across jurisdictions, actors, procedures, and contexts? Which data rights are most frequently exercised? And which types of data rights are least appropriately addressed through existing regulation? Furthermore, are data rights being exercised equally among individual demographics? These questions endow the topic of data rights with intrinsic interest and broad significance, as achieving effective rights implementation will require an understanding of the current state of data rights enforcement.

Challenges in Enforcement of Data Protection Laws

Online information, especially information provided by users, is considered a top commodity in the web-fueled economy. Individuals willingly and thoughtlessly provide vast amounts of data, while local websites are supposed to enforce terms of use of foreign websites. India has resorted to do-nothing overzealousness about privacy and has therefore faced increasing chaos. How can a country with over 500 million Internet users protect its major assets—privacy and personal data against nefarious non-fair practices introduced by social networking sites, freely accessible public forums, and misuse by corporates in unwarranted e-marketing practices?

Protection against cyber crime is best handled as a concurrent subject as is done in developed democracies. However, such protection requires better

debate and articulation to be effective. Nevertheless, it is asserted that protecting privacy and personal data does not warrant new legislation but rather the amendment and strict enforcement of existing laws, bolstered by a better conceptual understanding of the phenomenon.

Resource Constraints

When it comes to an effective regime of protection against invasive information and surveillance technologies, resource constraints become a challenge, if not fatal, to the success of the regime. These constraints could be at various levels such as human, financial, technical, political and jurisdictional (Basu, 2012). First, a successful regime will require knowledgeable personnel grounded in the application and enforcement of rules and regulations. Another requirement will be a firm infrastructure capable of supporting privacy laws through enforcement and a dedicated body to supervise, monitor and refine its application. Third, a firm regime will have a commitment by the government to make privacy protection an integral part of broader governance frameworks as any compromise of such governance may be invited on the pretext of protecting, or surveilling for, security (Sood, 2015).

Fourth, multi-jurisdictional issues will need to be resolved and cooperation of online corporate entities will require more than legislative orders or financial threat. Fifth, in the world where freedom and security, privacy and policing are collaterals and are most sought countries such as India will always remain a soft state and every step given to protect privacy will be challenged by security arguments. These are not afterthoughts or irrelevant beside-the-point challenges but are core issues facing India's privacy regime, warranting urgent attention and discussion. The combination of a technically-savvy and politically-informed populous has favoured the development of digital rights in the developing world. On the whole, political governments have avoided sci-tech backlashes from home-grown technologies on a basis of non-interference.

However, this has resulted in the absence of a counterbalance against extreme corporate power that have a vested interest in controlling future science and technologies relating to privacy, genetic engineering, information consumption and generation. Ultimately, given the fact that privacy is a moving target and meritocracy will never be an all-around peaceful solution, there is the question how well each side of the marketing process can respond with fair adjustment to unpredictable technology-induced disputes.

Impact of Data Breaches on Individuals

In today's increasingly connected world, personal data are collected, used, and shared by entities large and small, individuals and institutions alike. Individuals' personal data have become the preferred currency for online services and usually this exchange is free. Still, a growing chorus of graduates, researchers, practitioners, and media organizations increasingly highlights invasive and reckless practices in the data economy. Digital surveillance has come to characterize many aspects of modern life and it has been caught abusing old systems and processes. Almost 390 million customers and account holders in the U.S. have been affected by a data breach since 2006. The growing sophistication, scale, speed, and impact of unauthorized access to sensitive personal data and other network security breaches constitute market failures that the free market recommends for regulation (L. Mills & Harclerode, 2018).

Psychological and Financial Consequences

Rising public concern about privacy abuses, large-scale data sharing, and increasingly intrusive online practices, particularly related to technology-based aspects of daily life, have motivated growing calls for stricter accountability measures for large internet platforms (Bondre et al., 2021). Alongside these concerns, the Covid-19 pandemic coincided with the rapid growth of online services heavily reliant on personal and behavioral data. There is therefore an opportunity to examine whether behavioral behavior across these platforms is consistent with larger policy considerations about ethical data subject rights and whether ongoing discussions about particular incidents or actors are unifying.

While the idea of "the right to be forgotten" (RTBF) has received the most widespread attention as part of the GDPR, the regulation outlines tighter constraints relative to user data and greater rights to algorithm understanding, explanation, and repercussions. Nevertheless, the enforcement of these rights is still in its infancy, and no nation yet offers the same protections as the GDPR. Moreover, it is understood that this sort of regulation on its own does not guarantee user data protection. A more inconvenient truth is that platforms may willingly enhance anti-competitive practices and harm data subject rights as they mature without external incentives to remain reasonably accountable. Nevertheless, constraints need not be purely punitive. More impactful regulation may be able to steer the trajectory of an industry toward preferred outcomes while retaining a multiplicity of actors and approaches. In amici briefs issued ahead of

the recent Supreme Court case on the right to be forgotten, noteworthy and notable privacy advocates argued that data protection could enhance the quality of knowledge production by enabling Q&A systems in news aggregative contexts.

The Role of Startups in the Data Economy

With the opening of data and massive data explosion, data has become the most important production factor alongside capital, land and labour. Governments and firms in both developing and developed countries have been clamouring to vigorously develop their own big data economy. In India, thousands of startups focusing on data collection, analysis and quasi-data brokering, particularly personal data brokering have mushroomed. As new comers of the digital economy, Indian startups are generally smaller in size and experience and therefore, likely feature data disadvantage towards larger, more resourceful and better reputed firms or incumbents. This leads to data privacy and data protection issues.

While the situations Indian startups face are similar to those of startups in other developing or under developed countries, the unique knowledge and socio-cultural immersions of these startups, are likely to greatly affect their approaches to data privacy and data protection. The consideration of data protection or privacy as disadvantages is also likely to be more profound in developing countries. While discussions have provided a number of insightful cases in the developed world, it still remains ambiguous: To what extent data protection and privacy frameworks or legal arrangements help or hinder the competition of Indian startups? And how do Indian startups cope with the challenges of data protection and privacy?.

Future Directions in Data Protection

Shifts towards datafication globally have revealed vulnerabilities in terms of the ongoing realization of human rights and civil liberties. Despite being seen as stealthy and transient, data is one of the most vital resources in the modern digital economy. Datafication has, however, acquired a negative connotation, indicating developments over time that impact society and peoples' lives in unexpected and often unanticipated negative ways. A wide range of practices associated with datafication — surveillance, privacy violation, social sorting, manipulation of behaviour, misinformation, and inequitable outcomes — have exacerbated existing inequalities and marginalized sections of society.

In short, trustworthiness has to be at the heart of datafication — in terms of all relevant actors being

prudent custodians of the data that they are collecting. This is especially vital for government actors collecting sensitive information as citizens are more vulnerable because they do not have options to opt-out. In principle, safety, security, and privacy are separate concerns. An open and transparent ecosystem is needed to elucidate and satisfy people's expectations in order to sustain the data economy in a way that is beneficial for humanity. This entails a trellising effort where individual rights are protected while innovation is enabled. This may mean reconceptualizing what it means for states to create and govern in order to avoid breaches of rights. Policy nuance is key. Foundational issues must be resolved first, and once the intentions of governments are rightly set, the devices of programmatic analysis can be questioned.

Potential Reforms in Legislation

Over the past decade, the public discourse on data protection and privacy in India has gained traction. The polar extremes of this discourse range from those who are overenthusiastic about the recent developments in technology and social media and are bent on posing data protection norms as archaic and antediluvian, while the others are sceptical of technology and are against any innovations that leverage technology over the fear of personal data breaches (Mann, 2015). Balancing the rights of an individual in terms of privacy and the protection of personal data, to be co-existing with the right to innovate and foster major economic growth from an entire industry which promises many times replicable revenue sources, is no easy task. The current regime in India with regard to online collection and processing of data is practically very vulnerable, porous and archaic. Essential legislation and enforcement mechanisms have not matured with the developments in the online world. Enactment of ITA 2000 is still seen as a watershed moment in India's entry into the Internet world, which was enacted more than a decade ago. However, the advancements in technology and the exponential growth

of the Internet in the past decade have left the conventional regime of online service delivery with many loopholes. Data privacy and protection has not been the prime concerns during the unplanned major developments with regard to the Internet in the past decade (M. Jr. Marsh, 2009). While the Indian Government is mulling over the enactment of a stricter data protection law, it is equally important to address loopholes in the existing laws in India which overlap with the domain of data privacy and protection.

Conclusion

The swift progress in science and technology has always served as an omen for the survival of humanity, giving rise to innovations, but only after a series of checklists. The extravagant use of technology has a price, too. Numerous critical issues related to the violation of individual rights fall under scrutiny while governing technology, especially in the digital sphere. The data-driven economy has led to benefits over innovation, enabling entities from the public and private sectors to intrude into individual rights, including an individual's right to privacy. The rephrasing of rights in a new era of technology has led the Supreme Court of India to examine data protection laws in the digital governance of government-initiated services. The Indian situation seems to deviate from other jurisdictions regulating data protection despite the endorsement of it as a human right. The analysis emphasizes the obstacles that have hampered the creation of privacy legislation despite multiple judicial pronouncements on the right to privacy. Besides that, the ambitions of the Digital India programme seem healthy for the nation's fledging economy driven by a blossoming information technology sector; however, implementing such programmes without a data protection framework seems asymmetric. This paper provides an elaborate analysis of the socially influencing factors, positioning the current situation in the context of privacy protection.

References :

- Basu, S. (2012). *Privacy Protection: A Tale of Two Cultures*. [PDF]
 Sood, G. (2015). *COMPARATIVE ANALYSIS OF CYBER PRIVACY LAW IN INDIA AND IN THE UNITED STATES OF AMERICA*. [PDF]
 Mann, J. (2015). *Small Steps for Congress, Huge Steps for Online Privacy*. [PDF]
 Tene, O. & Polonetsky, J. (2013). *Big Data for All: Privacy and User Control in the Age of Analytics*. [PDF]
 Humerick, M. (2018). *Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*. [PDF]
 F III Palmieri, N. (2019). *Data Protection in an Increasingly Globalized World*. [PDF]

- Birnhack, M. & Elkin-Koren, N. (2011). *Does Law Matter Online - Empirical Evidence on Privacy Law Compliance*. [PDF]
 Kulesza, J. (2012). *Walled Gardens of Privacy or "Binding Corporate Rules?": A Critical Look at International Protection of Online Privacy*. [PDF]
 Agrawal, P., Singh, A., Raghavan, M., Sharma, S., & Banerjee, S. (2020). *An operational architecture for privacy-by-design in public service applications*. [PDF]
 Crabtree, A., Urquhart, L., & Lodge, T. (2018). *Demonstrably doing accountability in the internet of things*. [PDF]
 Urquhart, L., Lodge, T., & Crabtree, A. (2018). *Demonstrably Doing Accountability in the Internet of Things*. [PDF]
 Kwon, Y., Corren, E., Munilla Garrido, G., Hoofnagle, C., & Song, D. (2023). *SoK: The Gap Between Data Rights Ideals and Reality*. [PDF]