International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Data Protection and Privacy as A Fundamental Right - An In-Depth Analysis of The European Union and India's Data Protection Legislation

Nandinee Singh

Amity Law School, Noida

Abstract

In the digital age, the protection of personal data and the right to privacy have emerged as paramount concerns, necessitating robust legal frameworks to safeguard these fundamental human rights. This paper embarks on a comprehensive study of data protection laws in two distinct jurisdictions, the European Union (EU) and India. By examining the EU's General Data Protection Regulation (GDPR), renowned for its stringent data protection standards, and juxtaposing it with India's evolving legal framework, particularly in light of the Supreme Court's landmark recognition of privacy as a fundamental right and the ongoing deliberations on the Digital Personal Data Protection Act (DPDPA), 2023, this research aims to unravel the complexities of legislating privacy in the digital era. Through a comparative analysis, the article highlights the similarities and divergences between the GDPR and the DPDP Act, evaluates the effectiveness of these frameworks in safeguarding privacy, and explores the challenges posed by technological advancements. Furthermore, it delves into the future of data protection laws. By integrating legal analysis with the theoretical underpinnings of privacy as a fundamental right, this research contributes to the global discourse on data protection, advocating for a dynamic legal landscape that aligns with the evolving nature of privacy threats in the digital world.

Keywords: Data Privacy, Intellectual Property, European Union, Right to Privacy, Privacy laws India

Introduction

The global data privacy landscape is a complicated patchwork of issues stemming from various threats, including corporate data breaches, unauthorized government surveillance, sophisticated big data analytics' manipulative powers, and social media's widespread influence. These difficulties have sparked a global dialogue on the vital need for comprehensive, robust data privacy laws. These regulations should be able to handle current issues while yet being adaptable enough to deal with future, unanticipated technology advancements. The cross-border nature of the digital economy and the pervasiveness of digital data have exposed significant weaknesses in the protection of individual privacy, necessitating a re-evaluation and revision of current legal frameworks. As a result, nations all over the world are trying to create and implement strict data protection laws at a critical juncture. These legal measures seek to protect an individual's inalienable right to privacy without impeding economic growth or innovation. In light of this, a thorough analysis of the ways in which various nations, most notably the European Union and India, strive to uphold a precarious balance between the protection of individual privacy rights and the need to

keep up with the swift pace of technological advancement provides important insights into the intricate and dynamic field of data protection and privacy law.[1]

These days, data is all around us and has a significant impact on our daily lives. Every online activity adds to an ever-growing digital archive of human activity, from the seemingly insignificant act of using a search engine like Google to the standard procedure of entering credit card information for online purchases. This occurrence highlights a crucial shift whereby data goes beyond its conventional function to become an indispensable resource within the context of the digital economy. With an estimated $200 billion in worth, the data business has grown into a profitable sector. Data brokers are the major players in this market; they are organizations with a focus on compiling personal data from several sources. These intermediaries carefully analyse this data to create comprehensive profiles of people, which they then market to advertising companies looking to sell to companies that want to sell more precisely targeted marketing campaigns. The monetization of personal data represents a significant change in the value and trading of information in the digital era.

But this data-centric economy has effects outside of the business world as well. Globally, governments have included data gathering and analysis into their operational toolkits, purportedly with the aim of improving public welfare. However, this approach frequently crosses the line into mass monitoring, which raises worries about the degradation of civil liberties and privacy. Global diplomacy has become more difficult due to governments using data as a tool of espionage, demonstrating the strategic usefulness of data in international relations.

Theoretical and Legal Foundation of the Right to Privacy

Foundational Concepts and Legal Balance

The concept of privacy encapsulates the condition in which an individual's personal life and decisions are shielded from unwarranted scrutiny and intrusion. This foundational right encompasses the expectation to be left undisturbed by others, signifying not a retreat from societal participation, but rather a boundary within which societal intrusion is minimal, provided that one's choices do not inflict harm upon others. Within the societal fabric, there occasionally arises a tension between two fundamental but potentially conflicting liberties - the freedom of speech and expression & privacy. This friction manifests when one individual's exercise of their right to information, underpinned by the freedom of speech, encroaches upon another's domain of privacy.[2]

The legal framework surrounding privacy seeks to delicately navigate between these two rights, striving for a balance that respects both the individual's confidentiality and the community's right to information. A poignant illustration of this delicate balance is found in the legal case referred to as Mr. X v. Hospital Z.[3] The petitioner contended that his right to privacy was breached when a hospital disclosed his HIV positive status to his fiancée, leading to dissolution of their impending marriage. The decision hinged on the principle that the right to privacy can be overridden in circumstances where the disclosure of personal information serves to protect the rights and freedoms of others. Specifically, in this instance, the court adjudicated that the hospital's disclosure was legally and morally defensible, given that it safeguarded the fiancée's right to be informed of a critical health risk that directly impacted her well-being.

[1] Goswami, Kishori. (2023). Laws regarding right to privacy of personal data in India. Indian Journal of Integrated Research in Law, 3(4), 1-9.
[2] Siddiqui, Dogra Ziya. (2022). Data privacy laws in India. Jus Corpus Law Journal, 2(4), 538-545.
[3] Civil Appeal 4641/1998.

The legal claims to privacy emanate from two principal sources. The first is rooted in common law principle of tort, which allows to seek redress and claim damages for any unlawful invasion of their privacy by another party. The second source of privacy rights is found within constitutional law, offering protection against unauthorized interference by the State. This protection is implicitly enshrined under Article 21. This dual foundation underscores the multifaceted nature of privacy rights, encompassing protection from both individual and state-level intrusions, thereby ensuring a holistic safeguarding of personal liberty and dignity.[4]

In the intricate tapestry of the Indian Constitution, the explicit acknowledgment of the right to privacy is conspicuously absent, a detail that has sparked extensive legal and philosophical debates over the years. The genesis of the discourse on incorporating the right to privacy as an intrinsic part of Fundamental Rights can be traced back to the spirited discussions of the Constituent Assembly, the august body tasked with drafting the Constitution.

The judicial landscape regarding the right to privacy began to take shape with landmark cases such as MP Sharma v. Satish Chandra.[5] This case presented an early challenge to the constitutionality of search and seizure operations, arguing that they violated an implicit right to privacy. However, the Supreme Court, adhering to a strict interpretation of the Constitution, concluded that in the absence of an explicit declaration of the right to privacy within Fundamental Rights, government's search & seizure powers would remain unfettered by such considerations.

A similar stance was evident in the 1962's Supreme Court decision in Kharak Singh v. State of Uttar Pradesh, where court reaffirmed that Constitution does not explicitly guarantee the right to privacy.[6] Nonetheless, this case is also notable for the dissenting opinion of Justice Subbarao, who diverged from the majority view by advocating for the recognition of right to privacy as an essential facet of personal liberty. His dissent highlighted a philosophical and jurisprudential counter-narrative that emphasized the intrinsic value of privacy in a democratic society, setting the stage for future legal debates on this fundamental issue.

The legal journey towards the recognition and elaboration of the right to privacy in India has been intricate and progressive, culminating in pivotal judgments that have shaped its current understanding and application. Beginning with Govind v. State of Madhya Pradesh, the Indian judiciary embarked on a nuanced exploration of privacy rights, acknowledging them within certain limits for the first time.[7] The court posited that while privacy claims hold validity, they are not absolute and can be overridden by compelling public interest under specific legal frameworks.

The narrative of privacy rights in India took a significant turn with the R. Rajagopal v. State of Tamil Nadu, often referred to as the 'Auto Shankar case'.[8] This landmark case brought the conflict between the right to privacy and freedom of the press into sharp focus. The crux of the matter lay in determining whether a publisher could disseminate a person's autobiography without their consent, within guise of press freedom as enshrined in Article 19, and whether such an act impinged upon the individual's right to privacy. The court's deliberation led to a nuanced verdict, affirming that individuals possess an inherent right to protect their privacy, and unauthorized publication of their life stories without consent was not

[4] *Supra* note 3.
[5] (1954) AIR 300.
[6] (1963) AIR 1295.
[7] (1975) AIR 1378.
[8] (1994) SCC (6) 632.

permissible. However, this right was not absolute and did not extend to information already in the public domain; hence, consent was not required for the publication of such public records.

The legal discourse on privacy reached a seminal moment with the case of Justice K.S. Puttaswamy (Retd.) v. Union of India, where a nine-judge bench was convened to thoroughly examine the relationship between privacy rights and fundamental rights.[9] This landmark judgment unequivocally recognized right to privacy as a natural, inherent right crucial to human dignity and an essential component of human existence. The court elucidated the dual aspects of privacy: a negative obligation on the State to refrain from undue interference in individuals' lives, and a positive obligation to actively protect privacy rights.

Drawing inspiration from international legal principles, such as the "reasonable expectation of privacy" concept from Katz v. United States,[10] the court adapted this doctrine to the Indian context, underscoring that privacy expectations vary with the context, being higher in personal spaces and less so in public arenas.[11] Nonetheless, this does not imply an absence of privacy in public spaces but indicates a variable threshold of privacy expectation.

Moreover, the judgment established that the right to privacy, while fundamental, is not unqualified. It can be subject to reasonable restrictions through lawful means, aimed at achieving a legitimate purpose in a non-arbitrary, fair, and proportionate manner. The court set forth three critical tests for evaluating the validity of laws that encroach upon privacy rights: legality (the need for a clear legal basis), necessity (the legitimate aim of the law), and proportionality (the balance between the means used and the goal sought). This judgment also had profound implications for prior legal precedents, overruling the MP Sharma case[12] and partially overruling the Kharak Singh case,[13] which had previously held that privacy was not protected under the fundamental rights. Through these judicial milestones, the right to privacy in India has been firmly entrenched as a fundamental right, intricately woven into the fabric of individual freedom and dignity yet balanced with the considerations of public interest and state security.

An Overview of India's and the EU's Data Protection Laws

The GDPR represents a pivotal piece of legislation within EU law, focusing on the protection of data and privacy across the EU and the European Economic Area (EEA). Beyond its primary objective of safeguarding personal data within these regions, the GDPR meticulously outlines the prerequisites for transfer of personal data outside of the EU and EEA, ensuring the global handling of such data adheres to stringent standards. Central to the ethos of the GDPR is the empowerment of EU citizens and residents with unprecedented control over their personal information. This regulation not only aims to return sovereignty over personal data back to individuals but also seeks to streamline the regulatory framework for businesses operating on an international scale by establishing a cohesive data protection landscape across the EU. This unification of data protection laws was achieved through the repeal of the 1995's Data Protection Directive (Directive 95/46/EC), with the GDPR coming into full effect on May 25, 2018.[14]

[9] WP (Civil) No 494/2012.
[10] [1967] 389 US 347.
[11] Distt. Registrar & Collector v. Canara Bank, Civil Appeal 6350-6374/1997.
[12] *Supra* note 6.
[13] *Supra* note 7.
[14] *GDPR vs. India's DPDPA: Analyzing the Data Protection Bill and Indian Data Protection Landscape*. (2023, September 30). Secure Privacy. Retrieved February 19, 2024, from https://secureprivacy.ai/blog/comparing-gdpr-dpdpa-data-protection-laws-eu-india.

Indian Facets of Data Privacy law

In parallel, India has embarked on its journey to fortify the privacy and protection of personal data with the introduction of DPDPA, which marks the country's inaugural comprehensive data protection legislation. Having successfully passed through both houses of the Indian Parliament in August 2023, the DPDPA is poised for implementation in the early months of 2024. This legislation is a testament to India's commitment to safeguarding the personal data of its citizens, setting a precedent for data privacy within the nation.

The legislative journey to the DPDPA began with the introduction of Data Protection Bill in 2019. This draft legislation underwent a series of amendments and revisions reflective of the evolving discourse on data protection, culminating in the passage of the DPDPA in 2023. The evolution from the Data Protection Bill to the DPDPA provides valuable insights into the Indian government's legislative process and its prioritization of data privacy. This progression underscores the critical elements and frameworks that have been adopted to ensure the protection of personal data within India.

Framework of GDPR and DPDPA

Since its inception in 2018, the GDPR has been lauded as the benchmark for data protection regulation, often referred to as the "gold standard". Its comprehensive and stringent approach serves as a reference point for countries and organizations worldwide striving to enhance their data protection practices. Compliance with GDPR is not merely a legal obligation but a crucial aspect of operational integrity for organizations, necessitating a thorough understanding of its provisions. Non-compliance carries the risk of substantial financial penalties, a regulatory stance that is mirrored in India's DPDPA. This shared emphasis on accountability and compliance underscores the global recognition of importance of data protection and privacy in today's digital age.[15]

The GDPR is crafted with the principal aim of empowering citizens and residents of the EU with greater control over their personal data. Its enactment harmonizes the data protection laws across all EU member states, thereby simplifying the regulatory landscape for businesses engaging in international operations within the EU. Moreover, it is designed to bolster the safeguarding of personal data against any form of unauthorized handling, including access, use, disclosure, or destruction. The GDPR casts a wide net in terms of its applicability, extending its reach to all entities involved in processing the personal data of individuals who are in the EU. This is irrespective of whether the processing organization is physically located within the EU or not, making its scope truly global.

Rights & Compliances

Under the GDPR, individuals (referred to as data subjects) are endowed with several rights aimed at increasing their autonomy over their personal data. The right to request that their personal data be erased (right to be forgotten), the right to object to or restrict the processing of their data, and the right to view their personal data are only a few of these rights. Entities that control or process personal data (data controllers and processors) are tasked with significant responsibilities under the GDPR. These responsibilities encompass adopting adequate security measures to protect personal data and promptly reporting any data breaches to the relevant supervisory authority, thereby ensuring accountability and transparency in data processing activities. Penalties for non-compliance with the GDPR are severe and

[15] *Indian Data Protection Law versus GDPR – A Comparison*. (2023, August 18). AZB Partners. Retrieved February 19, 2024, from https://www.azbpartners.com/bank/indian-data-protection-law-versus-gdpr-a-comparison/.

can reach up to 4% of the guilty organization's annual global revenue or €20 million, whichever is higher. The significance of following the regulation is highlighted by these sanctions.

The DPDPA sets out to protect the privacy of Indian citizens by ensuring their personal data is handled responsibly. It aims to empower individuals with control over their personal data while fostering an environment conducive to innovation and economic growth within the digital ecosystem of India. Similar to the GDPR, the DPDPA applies universally to any organization that processes the personal data of individuals located in India, disregarding the geographical location of such organizations. This inclusive approach ensures that the privacy rights of Indian citizens are respected and protected globally.

Conclusion

In an era marked by the relentless accumulation of data, there is a growing unease around the erosion of personal privacy. India stands at a critical juncture, necessitating the establishment of a comprehensive data protection infrastructure that adeptly navigates the complexities inherent in safeguarding privacy within the digital domain. Crafting such legislation demands from India not just the adoption of advanced techniques and approaches but also the formulation of nuanced strategies and policies. This legal scaffold must carefully mediate between the privacy expectations harboured by its citizens and the aspirations of corporations to harness the latest technological innovations for expansion.

The DPDPA integrates several core concepts and standards that echo those found in leading data regulation models, like those instituted by the EU. Despite this, the DPDPA's approach is notably more foundational. While its brevity and straightforwardness might enhance its accessibility, making it more appealing to businesses, broad in scope, and adaptable to rapid technological advancements, this simplicity could also be its Achilles' heel. It might render the DPDPA less equipped to address certain nuanced challenges. It is anticipated, therefore, that prior to its official enactment, the DPDPA will embrace certain benchmarks prevalent in international data protection statutes, including but not limited to data localization, data portability, and the right to be forgotten. The incorporation of these standards would significantly bolster the reassurances provided to Data Principals.

Moreover, the introduction of 'deemed consent' as a concept within the DPDPA marks a novel and as yet unproven approach in the landscape of data regulation, necessitating a period of observation to fully comprehend its ramifications. Nonetheless, the DPDP is fundamentally in sync with the key principles underpinning the majority of the world's data protection laws. More crucially, it represents a significant advance by the Indian government beyond the framework set by the existing Information Technology Act, which has shown inadequacies in safeguarding the rights of Data Principals effectively.