Page 273 - 279 **DOI:** *https://doij.org/10.10000/IJLSI.112516*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 2

2025

Bridging Borders in the Realm of Privacy: A Comparative Analysis of EU Data Protection Laws and India's Data Protection Bill 2023

AYUSHMAN KUMAR B.[1]

ABSTRACT

Data protection has emerged as one of the most pressing legal and policy concerns in the digital era. Governments worldwide are enacting and refining laws to safeguard individuals' personal data and ensure privacy protections. This paper presents a comparative analysis of the data protection frameworks in India and the European Union (EU), with a particular focus on the evolving legal landscapes, judicial interpretations, and academic discourse. By examining key statutory provisions, landmark judicial decisions, and scholarly opinions, this research highlights the similarities and differences in how each jurisdiction seeks to protect individual privacy while enabling the free will in the flow of information in the digital economy.

Keywords*: GDPR, European Union, DPDPA, KS Puttaswamy.*

I. INTRODUCTION

Data protection has emerged as one of the most pressing legal and policy concerns in the digital era. Governments worldwide are enacting and refining laws to safeguard individuals' personal data and ensure privacy protections. This paper presents a comparative analysis of the data protection frameworks in India and the European Union (EU), with a particular focus on the evolving legal landscapes, judicial interpretations, and academic discourse. By examining key statutory provisions, landmark judicial decisions, and scholarly opinions, this research highlights the similarities and differences in how each jurisdiction seeks to protect individual privacy while enabling the free will in the flow of information in the digital economy.

II. EVOLUTION OF LAWS IN THE EUROPEAN UNION & INDIA

The European Union's General Data Protection Regulation (GDPR), approved by the European Government on 14 April 2016 and came into force on 25 May 2018, is widely

[1] Author is a LL.M. student at School Of Law, RV University, India.

 [ISSN 2581-9453]

regarded as the gold standard for data protection. It imposes stringent obligations on both controllers and processors,, and applies extraterritorially under certain conditions. This is a legal framework that sets guidelines for the collection as well as processing of personal information of individuals within and outside the European Union. This set of guidelines had replaced the the EU Data protection Directive of 1995[2], as it faced many challenges such as Technological advancements outpaced the provisions prescribed in the directive and the member States interpreted and implemented the directive differently, creating inconsistencies. GDPR focuses on keeping businesses more transparent and in expanding the privacy rights of data subjects. Moreover, the GDPR underscored the principle of accountability, requiring data controllers to demonstrate compliance through documented processes, data protection impact assessments , and, in some cases, the appointment of data protection officers . The provisions under GDPR very well reflect the fact that it hs positioned 'privacy' as a fundamental right, highlighting the commitments made by the European Union.

The concept of data privacy being recognized by the law in India traces back to a very important petition filed by Justice K.S Puttaswamy less than a decade ago. The Indian Constitution does not explicitly list "privacy" as a fundamental right. However, following a series of judicial pronouncements culminating in the landmark case of *Justice K.S.*

> *Puttaswamy (Retd.) v. Union of India (2017)*[3], the Supreme Court of India unanimously recognized the right to privacy as an intrinsic part of Article 21 (right to life and personal liberty) of the constitution of India.

By passing the the judgment in this case, the apex court overturned cases of *Kharak Singh v. State of U.P. (1962)*[4] and *MP Sharma v. Satish Chandra (1954)*[5], which had cast doubt on the scope of the right to privacy as there was inconsistency in judicial view. The Puttaswamy decision overruled these older precedents, firmly grounding privacy as a constitutional right. Previous to the judgment passed in the Puttaswamy case, There was complete absence of a comprehensive law to govern data privacy and protection and citizens were more reliant on digital systems (Aadhaar, e-commerce, etc.) which had very much highlighted gaps in existing laws.

In contrast, the EU has a robust framework for privacy rights, primarily governed by the General Data Protection Regulation (GDPR), which came into effect in 2018. The GDPR

[2] 1995: EU Data Protection Directive (Directive 95/46/EC)
[3] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India)
[4] Kharak Singh v. State of U.P., (1964) 1 SCR 332 (India)
[5] M.P. Sharma v. Satish Chandra, (1954) SCR 1077 (India)

establishes comprehensive protections for personal data and enshrines individuals' rights regarding their information. The EU's legal approach is rooted in the Charter of Fundamental Rights, which explicitly recognizes the right to respect for private and family life (Article 7) and protects personal data (Article 8)[6]. The European Court of Justice (ECJ) has played a pivotal role in interpreting these rights. For example, in Google Spain SL v. Agencia Española de Protección de Datos[7], the court recognized the "right to be forgotten," allowing individuals to request the removal of personal information from search engine results under certain conditions. This decision reflects a proactive stance on privacy, emphasizing individual control over personal data.

The DPDPA provides for regulation of the processing of digital personal data, which includes both digitally collected personal data and non-digitally collected personal data that has been digitised. Although the DPDPA's definition of personal data is comparable to that found in the GDPR, it does not include personal data that is made publicly available by the data principal or by anyone else who is required by law to do so.

Throughout the years, since the judgement passed by the Supreme Court, India has made strides toward modernizing its data protection regime, moving from a patchwork of legislative provisions under the Information Technology (IT) Act, 2000[8] and its associated rules, to the proposed Digital Personal Data Protection Act, 2023[9], which preceded by the Personal Data Protection Bill, 2019.

In 2018, a committee headed by Justice B.N. Srikrishna was tasked to draft a comprehensive data protection framework and submitted its report in the form of *Personal Data Protection Bill, 2018*. The report was keenly awaited by all for its implications on data handling and processing practices by both Indian as well as foreign companies along with government departments. Nonetheless, this was seen as complex and potentially restrictive for businesses. The PDP Bill was introduced in Parliament as *Personal Data Protection Bill, 2019* and referred to a Joint Parliamentary Committee (JPC) for review. The JPC recommended extensive changes, resulting in the reintroduction of an updated version of the Bill.the bill was revised and introduced in the Lok Sabha. The parliamentary committee published a report, explaining the insufficiencies of the bill citing the need for a ‘‘comprehensive legal framework’’. The main reasons for this was that it granted broad exemptions to government agencies, allowing them

[6] Michał Rojszczak, After the GDPR: The New Age of Data Protection in the EU – An Analysis, 24 Eur. L.J. 51 (2018).
[7] Google Spain SL v. Agencia Española de Protección de Datos, Case C-131/12, ECLI:EU:C:2014:317 (CJEU)
[8] Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India)
[9] Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India)

to access personal data without consent for vaguely defined reasons like "national security" and "public order" and that the fiduciaries were only required to report breaches likely to cause harm, potentially leading to under-reporting of incidents. Consequently, the bill was withdrawn in 2022. *The Digital Personal Data Protection Bill, 2023* was passed by both Houses of Parliament in August 2023 and received Presidential assent, becoming a statute.[10] Earlier versions of the bills were considered overly complex and bureaucratic, with detailed provisions that made compliance challenging. As a solution, The Digital Personal Data Protection Act, 2023, focuses on simplicity, covering only digital personal data while leaving non-personal data and sectoral specifics for future legislation.

III. BURNING ISSUES OF THE DPDP BILL

The bill of 2023 has also drawn upon some pressing concerns that can hinder the very concept of data privacy among us, the citizens of the country. The DPDP Bill gives the government the authority to notify any of its agencies that they have been provided exemption from the Bill for reasons such as maintaining public order or ensuring state security.Put another way, any government entity that is excluded from the DPDP Bill is free to gather and use residents' personal information for any reason they choose, without having to adhere to any of the protections outlined in the bill. This broad discretionary power raises fears of excessive data collection and retention, potentially leading to a surveillance state. The lack of clear guidelines or oversight mechanisms for these exemptions further exacerbates the risk of misuse.[11]

Furthermore, Section 36 of the bill gives the government the authority to request personal information from private businesses "for purposes of this Act," which is not a defined expression and can be used sometimes in an arbitrary manner. There is also an automatic exemption for processing personal data for the prevention, investigation, etc., of crime, without the need for the government to issue any notification. It is quite odd that a notice is required even when processing information for law enforcement. This basically implies that all offenders must to be informed in advance that their data is being monitored. Since the government has an obligation to protect its residents, it is legitimate for it to have the authority to keep information, including private information, that belongs to the people.

[10] Protection Act 2023 vs. the GDPR: A Comparison, Global Privacy Blog (Dec. 2023), https://www.globalprivacyblog.com/2023/12/indias-digital-personal-data-protection-act-2023-vs-the-gdpr-a-comparison/ accessed 21 January 2025

[11] Bhoomika Nanda, Critical Review of Digital Data Protection Act, 20, 2 Int'l J.L. Rsch. & Analysis 14 (2024), https://www.doi-ds.org/doilink/09.2024-86638611

According to Clause 3(c)(ii) of the bill, it won't apply to user-provided personal information.For instance, the Bill demonstrated that processing of personal data will not be covered by the data protection law if a person publicly shares her personal information on social media while writing her opinions.This enables businesses to handle publicly

accessible personal data without obtaining authorisation or abiding by any other Bill rules. For instance, in order to train their models, AI services like as Google Bard and OpenAI's ChatGPT will be allowed to scrape publicly accessible personal data from the internet.

Hence, this shall act like a free ticket for scraping of publicly shared personal data.

When it comes to the criteria of age, Companies that process the data of children , defined as anybody under the age of 18 are subject to additional requirements under the DPDP Bill.The DPDPA has provisions for the protection of children's data, but the government has been given excessive powers to prescribe exemptions in accordance with the DPDPA. Lacking clear guidelines for such exemptions the protection provided to minors could be eroded to leave their data susceptible to being used or exploited. Crucially, it mandates that before processing children's data, these businesses obtain "verifiable consent" from parents. In addition to depriving teenagers of agency by limiting their access to websites without parental consent, this places businesses in a difficult position because they will need to verify the age of all of their users, which would require gathering personal information like government-issued identification documents, in order to make sure they are not gathering any child's personal information without permission. According to the Bill, certain businesses may be exempt or have a reduced age requirement if they handle children's data in a manner that is "verifiably safe." However, it is rather unclear what qualifies for this requirement, and it establishes two distinct rules for businesses handling children's data. The Bill should use a graduated approach since a seventeen-year-old and an eight-year-old shouldn't be treated equally, in the same approach.

The power of the Government to block content goes beyond Section 69A of the Information Technology Act. According to Section 37 of the DPDP bill, if an entity commits repeated crimes or if it is in the "interests of the general public," the government may prohibit access to websites or content on the recommendation of the Data Protection Board . This expansive interpretation extends the government's already contentious authority to censor content under section 69A of the Information Technology Act of 2000. Furthermore, since a Data Protection Board is tasked with matters pertaining to data protection and "content" is a more of a general topic that is already covered by other laws like the IT Act, the Board's authority to advise on

restricting "content" shall be problematic.

Compensation for victims of personal data breaches is another big gap in the DPDPA. As provided by the Act, the breach is penalised with substantial penalties but this does not guarantee that those affected receive any form of compensation. Such omission neglects the direct harm felt by victims of data breach, and may not be adequate to incentivize organizations to prioritise data protection. Moreover, The establishment of the Data Protection Board creates questions on its independence and functionality. The Act giveth the Central Government the power to, inter alia, appoint the Board's Chairperson and Members which could go to compromise of its autonomy. Conflicts of interest are possible in this arrangement and particularly so when our data collection activities are government data processing. Because appointments are short term and there is a possibility of governmental influence, the Board lacks ability to act impartially.

It has also been noticed that somewhat weakens the Right To Information Act by giving the government more reasons to deny information. The RTI Act of 2005 is amended by the DPDP Bill to declare that the government is not required to reveal information pertaining to personal data. In the past, this may be disregarded if there was more public interest. The Bill weakens the RTI Act by adding this change, which gives the government another wide justification to refuse requests for information.

Some exceptions are made for the processing of personal data for the purposes of debt recovery. To take another example, borrowing a loan from a bank and failing to pay for the monthly instalment, the bank will retrieve the personal data of the person to check out their financial data regarding assets and liabilities. This can be a problem when there are no safeguards in place and indeed we are regularly seeing fake loan apps engage in unethical recovery practices of accessing contact lists and photo libraries of borrowers to threaten such borrowers with this personal data.Specific forms of data including health, biometric or financial personal data require more stringent conditions regarding processing and storing.Earlier iterations of the bill were sensitive and critical personal data sets treated as subsets of personal data subject to additional safeguards.ults on their monthly instalment, the bank may process the personal data of the individual to ascertain their financial information and assets and liabilities.

Without any safeguards, this can be problematic as we frequently see instances of fake loan apps engaging in unethical recovery practices by accessing contact lists and photo libraries of borrowers and blackmailing them using this personal data. Certain types of data such as health,

biometric or financial personal data merit stricter conditions for processing and storing. Earlier iterations of the bill had sensitive and critical personal data as subsets of personal data that were subject to additional safeguards. There are no such classifications in this bill.

IV. CONCLUSION

In the form of a genesis, The 1995 Data Protection Directive kicked off the EU's goal to achieve full coverage of data protection rules on the territory of the entire space of the Union. But as technology moved quick smart advances, there was a need for a more robust and unitary framework that sometimes turns into a decade long process of drafting which brought the General Data Protection Regulation into fruition.

India's path to data protection legislation has been more recent but no less complex. The DPDP Act, while drawing inspiration from the GDPR, has been tailored to India's unique context. However, under the same roof, Uncertainty and the risk of misuse of the Data Protection Board were created by the ambiguities which are connected to the independence of the Data Protection Board and overreliance on delegated legislation. At the same time the Act does not go far enough to protect children's data, there is also limited scope for the regulator to play a role in adapting to future challenges. To fill these gaps, the Act needs to be modified to detail more specific classification of the data, to strengthen one's rights, to specify the security standards, and to assure the agency's independence. Different methods of compensating for data breach victims and SMEs in compliance efforts are also contemplated. To realise the true promise of comprehensive data protection for Indian citizens in the digital age, only these drawbacks can be addressed.

*****