LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S6(2025)

COMPARATIVE ANALYSIS OF DATA PROTECTION AND PRIVACY LAWS

Mr. M Laxmi Jagannadh[1], Prof. (Dr.) S Sumitra[2]

[1]Research Scholar, Dr. B R Ambedkar College of Law, Andhra University
[2]Professor of Law, Dr. B R Ambedkar College of Law, Andhra University

Introduction

The advent of digital technology has made privacy central to regulatory debates, especially whether or not it should be safeguarded as a fundamental human right. Personal data, as such, has changed into digital formats, with new forms of infrastructure for surveillance, how information or data is shared through cross-borders and technology strictly targeted at analysing data. Personal data needs to be protected because it provides the basis or rationale for advancing politics and ideologies. This implies that privacy is getting a new definition, not only protectionist rights, but equally prioritising "freedom, dignity and autonomy" from authority's arbitrary interference. The digital age has seen privacy taking a whole new meaning, especially how it shapes the interactions between individuals and corporations or states as the world continued to become extensively globalised [1]. Governments and private corporations collect large amounts of data, making it crucial to protect the same from intrusive practices.

Different regimes have laws and regulation in privacy and data protection, which demands an extensive comparison. India, for instance, introduced the Digital Personal Data Protection Act, DPDP Act, 2023, seeking to balance personal privacy and innovation[2]. This new law can be compared with developed nations and regions like the European Union (EU) with its "General Data Protection Regulation (GDPR)" and the UK's equally similar model. This comparison also considers the United States sectorial approach and extensively assesses India relative to fellow BRICS. In so doing, engaging in comparative analysis provides the rationale for assessing evolving regimes, especially countries like India, and explaining how it has aligned or deviated from recommended international standards, especially the GDPR's provisions.

Theoretical Framework

Right to Privacy Philosophy

The concept of "the right to privacy" can be philosophically traced back to democratic and liberal traditions where "personal autonomy, human dignity, and the individual's moral worth" are emphasised[3]. Privacy heavily borrows from the concept of "liberty" as earlier coined by John Stuart Mills. Furthermore, in 1890, Samuel and Louis Brandeis articulated or framed privacy as "the right to be let alone", which has been the basis for contemporary intellectual basis for regulations and laws on privacy[4]. Accordingly, the "informal self-determination" was later coined by Alan Westin, leading to the evolution of the concept, where, providing individuals control over their personal data becomes central[5].

---

[1] Neil M Richards, 'Why Privacy Matters: An Introduction' [2021] SSRN Electronic Journal.

[2] Ministry of Law and Justice. , 'The Digital Personal Data Protection Act, 2023.' (16 November 2023) <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>.

[3] Neil M Richards, 'Why Privacy Matters: An Introduction' [2021] SSRN Electronic Journal.

[4] Sohail Aftab, Comparative Perspectives on the Right to Privacy (Springer Nature (Netherlands) 2024).

[5]Gamal Elkoumy and others, 'Privacy and Confidentiality in Process Mining: Threats and Research Challenges' (2022) 13 ACM Transactions on Management Information Systems 1.

Privacy has changed with the proliferation of digital technology, where physical spaces is no longer the focus and concern of protection. Rather, the protection has extended to controlling or protecting digital identities and how the same data is being used for behavioural influences. Consequently, contemporary scholars have had a new perspective of privacy, which they consider as a multidimensional construct involving aspects like "decision, information, and association"[6]. The notion and understanding informs contemporary data protection laws, with the moral right to individual right translated into legal rights that can be enforced. As such, the same has limited how those who control and process data handle individual or personal information.

Definitions

Data protection and privacy are seemingly related concepts, but unique and distinct conceptually. The term privacy, as such, defines the broader human right intended at safeguarding individuals from unwanted intrusion by private or state entities. This is different from data protection, outlining the institutional and legal mechanisms for enforcing the privacy of information by regulating the "collection, processing, storage and sharing" of personal data[7]. According to EU's GDPR, the term "personal data" implies any information associated to an identifiable or identified natural person. Accordingly, the body defines "processing" as any performed operation, like data[8]. A similar definition can be coined from DPDP Act, where the Indian version conceptualised "personal data" as an identifiable individual's digitally processed data. Conversely, DPDP Act defines "data fiduciaries" as entities determining the purpose as well as the means of processing[9]. From these definitions, they all high the differences in conceptualising control, accountability and consent within the digital context or environment.

India's Privacy Landscape

Constitutional Foundations of the Right to Privacy

Justice K. S. Puttaswamy (Retd.) v. Union of India (2017) became the landmark ruling that established India's recognition of individual's rights to privacy. This came out as a unanimous court ruling on the intrinsic nature of privacy as guaranteed under the Constitution of India's Article 21 guarantee on right to life and personal liberty[10]. Emphasised during this judgment was dignity and autonomy was the basis for informational privacy, with the state obligated to ensure citizenry's protection from both the government and private entities. The basis would become the country's normative formative for comprehensive data enactment as part of protectionist legislation.

DPDP Act 2023 and Regulatory Gaps

India enacted DPDP Act as the first of a kind to comprehensively regulate how digital personal data is collected and used. This is an act targeting to digital processing of data within the Indian jurisdiction as well as any entity involved in data processing beyond Indian when related to individuals providing goods and services in India[11]. Under this Act, key principles are

[6] Neil M Richards, 'Why Privacy Matters: An Introduction' [2021] SSRN Electronic Journal.

[7] Gamal Elkoumy and others, 'Privacy and Confidentiality in Process Mining: Threats and Research Challenges' (2022).

[8] European Commission, 'Data Protection' (commission.europa.eu2024).

[9] Ministry of Law and Justice. , 'The Digital Personal Data Protection Act, 2023.'

[10] Supreme Court of India, 'Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.'

[11] Ministry of Law and Justice. , 'The Digital Personal Data Protection Act, 2023.'

established to safeguard and guide the use or processing of such data, including "data minimization, purpose limitation, accountability, and consent".

Under the Act, "data principals," a term used to refer to individuals, are granted the fundamental rights to "access, correct, erase and grievance redressal." Following the Act, the Data Protection Board of India" was given the mandate to enforce the law, specifically slapping violators with a maximum of ₹250 crore in penalties[12]. Despite its intended focus and efforts at safeguarding privacy, several gaps have emerged from scholarly analysis. First, "digital" data is its limited scope, where physical records have been exclude. Through the provisions, the board can exempt state agencies on public order and national security grounds[13]. The uncertainty of the board is equally a concern, given that the central government is the appointing authority.

The provision on cross-border transfer of data renders the DPDP Act vague, with critical details left to subordinate rulemaking. The Act does not match the explicit provisions of the GDPR that clearly provides specific decisions and standard contractual clauses. Instead, the central government, under the Indian law, has the overall authority to notify the permissible jurisdictions without clear criteria specifying the procedure or such basis[14]. Similarly, the law has come under the scrutiny of critics who challenge that the law's features promote executive overreach, further weakening the privacy protection rights or provisions permissible tot the citizens.

Comparative Analysis

The India's privacy framework's strengths and limitations are better evaluated by through a comparative analysis with other data protection jurisdictions or regimes. Comparatively, the US, UK and EU alongside other BRICs countries provide the benchmark and template for evaluating the framework. The extensive comparison is because of the regimes' differences in different contexts and realms, including "regulatory scope, constitutional bases, and mechanisms for enforcement".

The European Union

In 2018, the EU enacted GDPR, which has since been the benchmark for protecting data globally. Under this act, data protection is considered as a fundamental human right as established under "The Charter of Fundamental Rights of the European Union's Article 8". Accordingly, there is extraterritorial application of the GDPR to any entity involved in personal data processing of EU citizens or residents, irrespective of the location of the establishment.

Accordingly, "personal" data under the GDPR is a broader term, but increased data protection targets ethnic, biometrics and health" data as "special categories." The framework also urges for a "freely given, specified, informed and unambiguous" informed consent. As a result, extensive rights have been directed or allowed at individuals, including "portability, erasure, rectification, access, and automated decision-making objection". The European Data Protection Board (EDPB) coordinate the supervisory authorities, ensuring that member states have uniformly enforced the law. Up to €20 million are charged as administrative fines. Cross-border

[12] Usha Tandon and Neeral Kumar Gupta, 'Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023' (2025) 6 Legal Issues in the Digital Age 87

[13] Soumyabrata Chakraborty, 'India's Data Protection Act Is More about the Processing of Personal Data than It Is about Privacy'

[14] Usha Tandon and Neeral Kumar Gupta, 'Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023' (2025) 6 Legal Issues in the Digital Age 87

transfer of data have also been targeted with stringent conditions, only permissible to states with "adequate" protections or "under standard contractual clauses" [15].

The United Kingdom

The UK retained, through its Data Protection Act 2018, retained the GDPR after Brexit, with the resulting "the UK GDPR" formed[16]. This mostly replicated the EU model, with provided or permitted rights including "access, erasure, rectification, restriction of processing and portability." Independent regulation is under "the Information Commissioner's Officer (ICO)", empowered to fine a maximum of £17.5 for violations. Yet, there has been a recent proposal by the UK government to make extensive reforms, with "data protection simplification" driving such efforts, although protection dilution concerns have been raised by experts[17]. Still, the UK GDPR is mostly aligned with the EU model irrespective of the new developments, majorly a rights-based regime

The United States

In the United States, there is no unitary comprehensive federal data protection law, instead using state-specific and patchwork sectorial statues. Privacy protection is limitedly protected under the Fourth Amendment, mostly targeting the protection against government surveillance. However, specific areas are protection using sectorial laws like the "Children Online Privacy Protection Act (COPPA)" and "the Health Insurance Portability and Accountability Act (HIPAA)"[18].

The California Consumer Privacy (CCPA) is the leading state-level data protection legislation. Recently, the California Privacy Rights Act (CPRA) was enacted with expansive consumer rights to "deletion, access, and opt-out of data sale"[19]. The California Privacy Protection (CPPA) operates as the enforcement authority alongside state attorneys general. However, this model is predominantly fragmented, with consumer protection prioritised, not using a universal rights-based approach. Accordingly, opt-out consent mechanisms are advanced rather than opt-in, with sectors or states having limited uniformity.

BRICS

Brazil is one of the BRICS with regulatory safeguards using its "Lei general de Protecao de Dados (LGPD)" where the same GDPR principles are evident. The "Protection of Personal Information (POPIA)" guides South Africa in protecting such rights, as China depends on "Personal Information Protection (PIPL)". China and Russia, however, are unique cases with their prioritisation of "sovereignty and state surveillance." These countries ensure that at the local levels, there are stringent safeguards, but state powers are broadly expanding on how personal data can be accessed[20]. Overall, data governance is a shared commitment among BRICS nations, although significant differences exist in balancing state interests and individual rights

Comparative Parameters

The cross-regime comparative reviews reveals sharply contrasting approaches to balancing institutional control and individual right based on different parameters. For instance,

[15] European Commission, 'Data Protection' (commission.europa.eu2024)

[16] ICO, 'UK GDPR Guidance and Resources' (ico.org.uk2023)

[17] Matthew Holman, 'Toothless Watchdog Means We Should All Worry about Digital IDs'

[18] Fred H Cate and Viktor Mayer-Schönberger, "Notice and Consent in a World of Big Data," Digital Repository @ Maurer Law, 2018,

[19] State of California Department of Justice, "California Consumer Privacy Act (CCPA),"

[20] Christopher Kuner, "Transborder Data Flows and Data Privacy Law," May 9, 2013,

the Indian and EU models constitutionally considers privacy as an underlying "fundamental right"[21]. The only difference with the EU is that data protection has been explicitly attached to the "Charter of Fundamental Rights", ensuring a stronger legal protection or certainly. However, the US model does not have a clear privacy clause in the constitution, mostly depending on the interpretations by statutes and jurisprudence[22]. There are widely varying constitutional guarantees with the BRICS, where some nations prioritise national security over individual privacy.

The UK GDPR and GDPR, based on scope, incorporates all personal data forms, whether offline or online. Nonetheless, the DPDP Act, the Indian version, is only confined to protecting or safeguarding digital personal data[23]. Based on the limitation, there is a glaring limitation with the India's protection framework. This is because categories of sensitive data existing in physical formats are largely excluded.

Another area of comparison is on definitions. For instance, the GDPR clearly distinguishes "special categories, processing and personal data", a consideration that has guaranteed consistency and accuracy[24]. The DPDP Act was designed based on the same structure and format. However, the Indian Act has not explicitly defined or classified sensitive personal data and is equally limited by its heavy reliance on rulemaking by the government when defining these key terms.

There is also a markedly difference in consent standards. The GDPR requires "informed, explicit and freely given consent," whereby the controller must provide the "burden of proof". Similarly "specific, free, unambiguous, and informed" consent is obligated by the DPDP Act. Conversely, there are "legitimate use" clauses introduced where consent may not be required when processing data, like obligations to comply or state functional requirements[25]. The additional provision has been challenged for threatening informed consent.

In next aspects of comparison, "data subject rights" should be considered. For instance, the UK and EU frameworks have allowed broader entitlements, especially portability of data and how individuals can object automated processing of their personal data. Fewer rights have been allowed under the DPDP Act, with data portability not directly protected. Data subject rights vary in the US based on the legislation of the state, although the more comprehensive provisions exist in California.

There are divergent data protection independence and effectiveness in different regimes. The supervisory authorities in the EU largely work independently and have "extensive investigative and corrective powers". In the UK, the ICO is an independent authority acting without government interference[26]. However, there is no central authority controlling the US's data protection regime. In India, although still in the formative stage, the Data Protection Board

[21] Matthew Holman, "Toothless Watchdog Means We Should All Worry about Digital IDs,"

[22] Fred H Cate and Viktor Mayer-Schönberger, "Notice and Consent in a World of Big Data," Digital Repository @ Maurer Law, 2018,

[23] Soumyabrata Chakraborty, "India's Data Protection Act Is More about the Processing of Personal Data than It Is about Privacy,"

[24] ICO, "UK GDPR Guidance and Resources," ico.org.uk, 2023,

[25] Ministry of Law and Justice. , "The Digital Personal Data Protection Act, 2023.

[26] ICO, "UK GDPR Guidance and Resources,"

oversees such operations, although its independence is questionable given that the government is still the appointing authority.

The data protection regimes differ in how data transfers happen in cross-border. For instance, the GDPR has stipulated clear guidelines and restricted exchanges or transfers to only where the protection level is deemed "adequate". Conversely, the DPDP Act is a provision ensuring that the government can identify data transfers countries[27]. However, uncertainty emerges with limited clear criteria for adequacy or oversight provisions.

There is also a dramatic variation in enforcement and penalties across the jurisdictions. Stringent fines exist in the EU, up to 4% global turnover, similarly followed by the Brazilian and the UK's tax regimes. A fine amounting to ₹250 crore or $30 million equivalent is charged under the DPDP Act, yet, it has not been tested on effectiveness of enforcement[28]. The US, however, has inconsistent penalties, with settlements used to determine such values. The final point of difference is on the litigation patterns. Specifically, the provisions are robustly enforced in the EU jurisdictions, with frequent judicial interpretations. India, however, still has a new privacy litigation.

Findings: India in Comparative Perspective

India's data protection framework, when comparatively evaluated and analysed, partially aligns with the recommended best global standards and practices. The DPDP Act's enactment was borrowed from most GDPR principles like "consent, purpose limitation, and individual rights" (GDPR, 2024). However, the Act's overall design has remained less comprehensive. A strong normative basis exists with its constitutional privacy recognition, yet, implementation of this statute is limited in various aspects. One of the major concerns relates to the scope, specifically "digital-only", undermining its reach. Therefore, there is lack of alignment or inconsistency between physical and data protection. Additionally, state exemptions are extensive regarding public order and national security, opposite to *Puttaswammy*'s proportionality principle. The third limitation is that the law has to be implemented in regards to the delegated legislation, further undermining its predictability and transparency. Besides, the executive control limits the "Data Protection Board's" autonomy.

By assessment, the data protection culture in India could be easily defined as promising, but still derailed by limited public understanding of such laws and protections. They have not established a groundwork of case laws as references for supporting this new provision. The approach is not focused on human rights or centres on the plight of citizens as stipulated by the GDPR model or framework [29]. Therefore, when care is not taken, the new law could promote a new framework that promotes surveillance and compliance over human rights protection. This means that the law may be implemented without necessarily considering the input of the public or proper regulatory safeguards and oversight.

Policy Recommendations

There are pros and cons with this India's renewed emphasis or new provisions for protecting privacy and personal data**.** Through the DPDP Act, the country has established a basis for data protection, showing a concerted effort towards meeting the global standards [30].

[27] Anirudh Burman, "Understanding India's New Data Protection Law,"

[28] GDPR, "General Data Protection Regulation (GDPR)," General Data Protection Regulation (GDPR), 2024,

[29] Soumyabrata Chakraborty, "India's Data Protection Act Is More about the Processing of Personal Data than It Is about Privacy,"

[30] Anirudh Burman, "Understanding India's New Data Protection Law," carnegieendowment.org, October 3, 2023,

However, with limited mechanisms for oversight and broad exemptions by the government, there are risks for disproportionate surveillance.

India should base its framework on privacy activism to balance weaknesses in regulation and institution. This involves collaborating with "civil society, digital rights advocates, and legal scholars" to improve awareness and champion for more accountability. Such collaboration will improve or ensure consistent interpretation of the DPDP Act[31]. Secondly, there is a need to prioritise judicial oversight, with the proportionality test mostly used by courts as outlined in the *Puttaswamy* to ensure necessary state surveillance that are equally proportionate and independently reviewed. Greater transparency will emerge with *post-facto* audits and surveillance requests prior authorised by the judiciary. Accordingly, the DPDP Act require robust policy reforms for including non-digital data, clearly establishing criteria for data transfers in cross-border and ensuring the Data Protection Board's independence is [32]. At best, the public needs more extensive education and awareness so that they can demand accountability.

Conclusion

From the comparative analysis, India made a significant milestone in data protection with its DPDP Act, 2023, but still at a budding stage and intermediately evolving. Unlike the highly established GDPR used in both the UK and EU, the India's law is plagued by broader discretion by the executive and weaker institutional independence. Additionally, it barely matches the fragmented model of the US, but still ensures a unified framework. The only concern is that this new law is devoid of a deep-embedded enforcement history and rights culture. When compared with the fellow BRICS countries, India exists between rights-oriented regime that Brazil uses and China and Russia's surveillance-based models. To succeed, the DPDP Act should be morphed into a comprehensive framework that protects privacy.

Bibliography

Aftab, Sohail. *Comparative Perspectives on the Right to Privacy*. *Ius Gentium*. Springer Nature (Netherlands), 2024. https://doi.org/10.1007/978-3-031-45575-9.

Burman, Anirudh. "Understanding India's New Data Protection Law." carnegieendowment.org, October 3, 2023. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en.

Cate, Fred H, and Viktor Mayer-Schönberger. "Notice and Consent in a World of Big Data." Digital Repository @ Maurer Law, 2018. https://www.repository.law.indiana.edu/facpub/2662?utm_source=www.repository.law.indiana.edu%2Ffacpub%2F2662&utm_medium=PDF&utm_campaign=PDFCoverPages.

Chakraborty, Soumyabrata. "India's Data Protection Act Is More about the Processing of Personal Data than It Is about Privacy." Jurist.org. - JURIST - Commentary - Legal News & Commentary, August 29, 2023. https://www.jurist.org/commentary/2023/08/indias-data-protection-act-is-more-about-the-processing-of-personal-data-than-it-is-about-privacy/.

Elkoumy, Gamal, Stephan A. Fahrenkrog-Petersen, Mohammadreza Fani Sani, Agnes Koschmider, Felix Mannhardt, Saskia Nuñez Von Voigt, Majid Rafiei, and Leopold Von Waldthausen. "Privacy and Confidentiality in Process Mining: Threats and Research

[31] Ministry of Law and Justice. , "The Digital Personal Data Protection Act, 2023.,".

[32] Anirudh Burman, "Understanding India's New Data Protection Law," carnegieendowment.org, October 3, 2023,

Challenges." *ACM Transactions on Management Information Systems* 13, no. 1 (March 31, 2022): 1–17.

Europa.eu. "EUR-Lex - 12016P/TXT - EN - EUR-Lex. Europa.eu," November 16, 2016. https://eur-lex.europa.eu/eli/treaty/char_2016/oj/eng.

European Commission. "Data Protection." commission.europa.eu, 2024. https://commission.europa.eu/law/law-topic/data-protection_en.

GDPR. "General Data Protection Regulation (GDPR)." General Data Protection Regulation (GDPR), 2024. https://gdpr-info.eu/issues/fines-penalties/.

Holman, Matthew. "Toothless Watchdog Means We Should All Worry about Digital IDs." Thetimes.com. The Times, October 2025. https://www.thetimes.com/uk/law/article/toothless-watchdog-digital-id-state-surveillance-gxv07gbcv.

ICO. "UK GDPR Guidance and Resources." ico.org.uk, 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

Kuner, Christopher. "Transborder Data Flows and Data Privacy Law," May 9, 2013. https://doi.org/10.1093/acprof:oso/9780199674619.001.0001.

Ministry of Law and Justice. "The Digital Personal Data Protection Act, 2023.," November 16, 2023. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf .

Richards, Neil M. "Why Privacy Matters: An Introduction." *SSRN Electronic Journal*, 2021. https://doi.org/10.2139/ssrn.3973131.

Santana, Paulo Campanha, and Faiz Ayat Ansari. "DATA PROTECTION and PRIVACY as a FUNDAMENTAL RIGHT: A COMPARATIVE STUDY of BRAZIL and INDIA." *Journal of Liberty and International Affairs* 9, no. 3 (2023): 456–70. https://www.ceeol.com/search/article-detail?id=1210587.

State of California Department of Justice. "California Consumer Privacy Act (CCPA)." State of California - Department of Justice - Office of the Attorney General, 2024. https://oag.ca.gov/privacy/ccpa.

———. "California Consumer Privacy Act (CCPA)." State of California - Department of Justice - Office of the Attorney General, 2024. https://oag.ca.gov/privacy/ccpa.

Supreme Court of India. "Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.," November 16, 2017.

Tandon, Usha, and Neeral Kumar Gupta. "Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023." *Legal Issues in the Digital Age* 6, no. 2 (July 2, 2025): 87–117. https://doi.org/10.17323/2713-2749.2025.2.87.117.