Page 1879 - 1886 **DOI:** *https://doij.org/10.10000/IJLMH.119258*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Privacy in Technology Innovation and the Challenges it Creates for Implementing the GDPR and India's DPDP Act

MANJUNATH RAVI HEGGADE D.[1]

ABSTRACT

The rapid advancement of technology, including Artificial Intelligence, Cloud Computing, Blockchain, and the Internet of Things, has introduced unprecedented challenges to data privacy and regulatory compliance. The European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act (DPDP Act) aim to safeguard individual privacy rights while fostering technological innovation. However, the evolving nature of digital ecosystems complicates their implementation.

This paper explores how emerging technologies challenge GDPR and DPDP Act compliance, particularly in areas such as data minimization, informed consent, automated decision-making, and cross-border data transfers. It examines the limitations of these regulations in addressing AI-driven data processing, profiling risks, and the black-box nature of algorithmic decision-making.

The study also evaluates the gaps in privacy-by-design principles, sector-specific governance, and accountability frameworks within these regulatory landscapes. Through a comparative analysis, the paper proposes solutions such as standardized consent management systems, transparency-enhancing mechanisms in AI models, and the integration of privacy-centric designs in technological innovations. By balancing regulatory compliance with digital transformation, this research aims to provide insights into fostering a privacy-conscious technological future.

***Keywords**: Blockchain, Cloud Computing, Internet of Things, Data Privacy, Compliance, Algorithmic Decision-Making, Cross-Border Data Transfers, Privacy by Design.*

I. INTRODUCTION

The European Union innovation of General Data Protection Regulatory (GDPR)[2] aims to bring strict regulatory provisions for protecting an individual data privacy in the European Union (EU) as well outside of EU. The rapid growing digitalization, technological innovations like Artificial Intelligence, Cloud computing, Internet of Things and extensive use of personal data

[1] Author is a LL.M student at RV University, Bengaluru, India.

[2] General Data Protection Regulation (GDPR) https://gdpr-info.eu/ accessed 24 January 2025.

 [ISSN 2581-5369]

by these technologies are threating privacy of an individual in digital age and usage of individual personal data poses a challenge in protecting and implementing of regulatory provisions of GDPR.

Similarly, in India, the Digital Personal Data Protection Act, 2023[3], the law to protect the privacy of an individual, faces a numerous challenge in protecting the interest of technical developments, after the landmark judgment by Supreme Court in Justice K S Puttaswamy case, held that Privacy is a fundamental right of an individual which is a part of basic structure of Indian constitution. However, increasing the use of technology and advancement of AI and IoT based data collection and processing are raised the concerns of misuse of individual sensitive data which is violation of an individual privacy. This paper tries to find out how technological innovations are creating the challenges for the implementation of GDPR in EU and India's DPDP.

II. PRIVACY REGULATIONS IN EUROPEAN UNION GDPR AND INDIA'S DPDP ACT

One of the prime objectives of GDPR is to protect the privacy of EU residents irrespective of citizenship and implementing the privacy regulations in its border as well beyond its border. GDPR strictly regulates the data processing organization and provides strict principles related to data collection and data processing of any organization whether it is technological driven or non-technical driven. If any organization fails to compliance with the regulations of GDPR that can lead to fines up to 4 % of annual turnover of that organization.

Whereas India's Digital Personal Data Protection Act aims to protect the privacy of an individual during data collection and data processing mechanism. The act provides provisions related to consent mechanism, processing and obligations to data fiduciaries to protect the principles of privacy, transparency and accountability. But the act fails to provides privacy protection outside the border of India.

(A) Technological Challenges of GDPR Compliance

The technological innovations like Artificial Intelligence, Cloud Computing, Blockchain, Internet of Things etc. are rising a concern of privacy of an individual in a data govern digital age. The GDPR and DPDP Act emphasize the data minimization principle. The objective of data minimization is to protect the privacy of an individual by collecting limited data which are essential for processing required purposes only. However, the application of this principle in AI driven machine is not satisfactory. The AI are programed which are not transparent due to its

[3] PRS Legislative Research, 'Digital Personal Data Protection Bill, 2023' https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 accessed 24 January 2025.

black box concept. The machine collects more data without knowing the individual which can use for various process in future without consent of an individual because AI driven machine relies on vast amounts of data to generate the outcomes to given prompt which indirectly violates the privacy of an individual and poses the challenges to implementation of GDPR and DPDP act data misuse. The emerging technologies[4] like Block Chain, Cloud Computing, the Internet of Things, Artificial Intelligence are posing compliance challenges with the European Union GDPR and also with the Indian DPDP act. These emerging technologies are good for innovation but at the same time challenge the individual privacy. The objective of the GDPR and DPDP acts is to ensure individual data protection and privacy in their respective countries, but the digital revolution and technological adoption raises the concern about privacy laws.

Blockchain Technology[5] is tech system in which it records information that is impossible to hack or change. Once data is stored, it can be transferred only by the owner's signature and authentication. It stores the transactional data in blocks in several databases like a chain. The Blockchain technology's inherent transparency aligns with the accountability principle of GDPR but is silent on provision of the right to erasure and rectification provisions of GDPR. In public blockchain technology, it lacks centralized control and makes data alteration impossible and creates issues of storage limitation provisions of GDPR. So, bringing the forgetting blockchains principle will allow the deletion of blocks and align with GDPR principles, offers greater compliance with GDRP provisions of right to erase.

Cloud computing[6] is a technology that uses hosted services in which data is stored on physical servers which are controlled and monitored by a cloud service provider. The data stored in the cloud is computable and transferable without direct management by the user. The GDPR provisions for data integrity and confidentiality are at risk due to security vulnerabilities in the cloud system. When data breaches occur and also, service level agreements, of cloud computing are vague in nature, which challenges the transparency regarding data processing with it creates issues of GDPR transparency and accountability principles. Cloud computing also raises the concern regarding the transfer of personal data between cloud providers, which affects the GDPR data portability principle. All the data is stored in cloud systems based on geographical distribution; complicated compliance with the right to erasure of data. So developing the rules related to complaint cloud architecture and enhancing service level agreement transparency

[4] Rania El-Gazzar and Karen Stendal, 'Examining How GDPR Challenges Emerging Technologies' (2020) 10 *Journal of Information Policy* 237.
[5] Zibin Zheng and others, 'An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends' (6th IEEE International Congress on Big Data, June 2017).
[6] Tanweer Alam, 'Cloud Computing and Its Role in the Information Technology' (2020) *SSRN Electronic Journal.*

could be a solution to accountability and data protection practices in cloud service technology.

The Internet of Things[7] is a technology which involves electronic devises and sensors through the connected internet. It processes the commands or prompts given by humans for required services in a simpler manner. It involves massive data collection, more than exceeding necessary. This clearly violates the GDPR's data minimization principle and also data limitation. The work of the Internet of things lacks transparency in data collection and processing, which undermines the principles of informed consent under article 6 of the GDPR. The IoT depends on decision analytics process and automated decision-making, which raises the concerns of discriminatory practices like bias, which violates the compliance of rights against automated decision-making under GDPR. So, bringing the robust mechanism for informed consent and data limitation to IoT technology process will solve the accountability and transparency challenges.

Artificial Intelligence technology, which solves the complex problems in second by its machine process thinking[8]. It creates creative solutions and outputs based on given prompts to the system. The AI machine outcomes are based on the process of available data sets, which leads to automated decisions. Here this leads to questions of fairness and accountability provisions of GDPR. The AI models fail to explain the logic behind its decision-making process and data collection, which violates fairness principles. So, adopting privacy by design approaches in AI models will enhance the transparency in the decision-making process and address the compliance gaps. So, balancing this innovation with the privacy of an individual will solve the implementations challenges to GDPR and DPDP act by balancing the innovations.

So technological Enablers and Solutions for GDPR compliance are suggested in the study, it emphasizes the adoption of information governance in technology organization for managing the data information will protect the organizational objectives and bridge the implementation of gap in GDPR. The challenges around consent are concern across technologies which need a standardize consent management systems so that it will improve the user interfaces with technology in transparent manner. Comparative studies on GDPR and other laws relates to data protection across the globe will identify the universal best practices for GDPR compliance with technology driven society. So ethical analysis of data laws shows that, need for a balance the privacy of an individual in line with technological innovation in the future.

[7] Zainab H Ali, Hesham Arafat Ali, and Mahmoud M Badawy, 'Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions' (2015) 128(1) *International Journal of Computer Applications* 975-8887.
[8] Katherine Quezada-Tavarez, Lidia Dutkiewicz, and Noémie Krack, 'Voicing Challenges: GDPR and AI Research' (2022) 2:126 *Open Research Europe*

 [ISSN 2581-5369]

III. TECHNOLOGICAL CHALLENGES OF INDIA'S DPDP ACT COMPLIANCE

The Digital Personal Data Protection Act of India primarily aims to address the protection of personal data in the digital driven and data-based world. It provides the rules and obligations to data fiduciaries who are collecting and processing the data of an individual for required purposes. The act aims to provides the protection provisions for individual privacy. The DPDP act provides strict provisions and includes principles similar to the EU GDPR, which mainly emphasize on transparency and consent validity. Principles like data minimization, purpose limitation, data subject rights, cross-border data transfers and obligations to data processors. The objective of India's DPDP is in line with GDPR principles and also aims in protecting an individual privacy, which is a fundamental right in the Indian constitution.

The technological innovations like artificial intelligence systems which work based on the data sets available in digital world or cloud system, which leads to a primary concern for individual data privacy. Artificial Intelligence often repurposes the data for unclear objectives without transparency[9], this makes the Act explicitly provides provision for data limitations but AI use of data is not clear and DPDP lacks the clarity on restricting reuse of data by AI systems or applications. So, solution is to make clear a guideline regarding reuse of data by AI systems or any technological driven system influence by the AI in order to protect the individual's privacy. The automated system technology poses challenges to the implementation of the DPDP act principles of transparency, and also the act lacks explicit provisions to control the misuses of data by automated decision machine driven by AI technology. To resolve this incorporation of detailed rules related to decision making process under the DPDP act will resolve the issues of transparency. The DPDP Act covers basic rights like correction of data and access to data, but it does not emphasize profiling related data this will make escape for AI decision making machine from the ambit of law, so bringing comprehensive provision to integrate AI decision should compliance with transparency provisions will strengthen the trust in innovation and ensure responsible AI technology development. The cross-border data transfers are not clear in the DPDP act with respect to AI applications this pose the challenges to bypass the provision of law which has to be consider and resolve.

India is an emerging economy with a growing hub for technological innovations like Artificial intelligence, this has raised the ethical challenges like fairness, accountability, transparency in that technology. So, bringing, the sector specific guidelines like AI ethics codes for alignment

[9] Pradip Kashyap, 'Digital Personal Data Protection Act, 2023: A New Light into the Data Protection and Privacy Law in India' (2024) *Teerthanker Mahaveer University.*

 [ISSN 2581-5369]

with DPDP provisions will resolve the non-discrimination issues. Both the GDPR and DPDP laws provide the provisions of privacy protection but both lack the clear boundaries on pervasive surveillance. Possible solutions for harmonizing technology innovation like AI under the India's DPDP act is, the act should expand the principles provisions to address the AI block box concept, algorithm biases and profiling practices. The guidelines should cover the reusing of data and also applications of machine learning in innovations. So, India's DPDP act still needs to evolve in to an AI ready framework like GDPR in order to support innovation while safeguarding the privacy of an individual and bringing trust in innovation.

(A) Modern Technology Innovations[10] Creating Challenges to Right to Privacy

Big Data dependent technology, particularly Artificial Intelligence systems depend more on vast data sets to generate the solutions to the user given prompt, which includes the sensitive data of an individual. For example, in the health sector, the AI driven autonomous health systems collect and store patient's sensitive data before the treatment process. Here rises the concern about how patient data is stored safe and monitored after the treatment. Both GDPR and DPDP act silently on big data usage, but provide data minimization principles which mandates the data processor to collect the data of an individual for specific purposes only in order to protect, their privacy.

The opaque nature of technology, the AI works on algorithms which are not visible to anyone due to black box code. This makes the AI systems make decisions based on invisible data sets, involves zero transparency and violates the privacy of an individual. For example, for loan approval processes, the software driven by an AI algorithm may misuse the data and give the results in a biased manner.

Privacy by design, the innovation in technology like AI, IoT, and autonomous vehicles often violates the privacy of an individual during the development stages. The European Union GDPR mandates the technology companies to follow privacy by default under Article 25[11]. In India's DPDP act advocates data protection measures, but it lacks the provision for privacy by design. So, when there are no provisions for privacy by design, it makes the technology developers prioritize their systems' function over privacy measures, it has to be resolve. Example; the internet of things devices collects data, but it lacks the clear privacy features or data eraser options of the devices that cost the user privacy.

[10] Ivana Stepanovic, 'Modern Technology and Challenges to Protection of the Right to Privacy' (2014) 62(3) *Anali Pravnog fakulteta u Beogradu* 167-178.
[11] Giorgia Bincoletto, 'Data Protection by Design: From Privacy by Design to Article 25 of the GDPR' in *Data Protection by Design in the E-Health Care Sector* (January 2021) 37-166

Bias related issues, AI technology uses data analytics which can create profiling or bias related issues. GDPR restricts the profiling without explicit consent from the user, but the DPDP act lacks the provision and rules to control technology profiling, so it might misuse the user data and cause the privacy concerns. Example software or apps used in the employment process often disadvantages the minority sections applications due to profiling of data.

IV. SOLUTIONS FOR NAVIGATING PRIVACY IN THE TECHNOLOGY ERA

Data Governance Frameworks, concerned government and regulators have to ensure data governance by bringing a robust governance frameworks which can accommodate the technological innovations without compromising the rights of individuals[12], especially privacy. So, solutions can be bringing the detailed sector specific rules or law for AI models and driven machines under the GDPR and DPDP Act will balance the privacy and technology, and also it requires the collaboration between the law makers, technology developers.

Transparency in AI working, bringing the regulations with respect to transparency in AI analytics and adopting the provisions of promoting sensitivity analysis to mitigate the hidden biases in AI applications will results trust in AI outcomes. The best example is that credit scores are given by a company which is based on AI-driven analytics, it can be bias so bringing the transparency by providing an explanation of how AI software data is processed before giving the Credit score result.

Integrating privacy in design, in this technology, developers and companies have to integrate privacy principles in every stage of development[13] this will ensure the privacy compliance while fostering innovation. And additionally giving tax incentives to the technological developers who integrate privacy in their innovation will results balance in privacy principles with innovations.

Public awareness is also an important factor in which individuals will get to know about their rights when technology misuses, which should be consider under the GDPR and DPDP Act. Along with awareness can be achieved by conducting mass education to the public through a campaign.

[12] Karl D Schubert and David Barrett, 'Data Governance, Privacy, and Ethics' in *Human Privacy in Virtual and Physical Worlds* (May 2024) 87-110

[13] Vasiliki Diamantopoulou and Maria Karyda, 'Integrating Privacy-by-Design with Business Process Redesign' in *Computer Security: ESORICS 2021 International Workshops* (Lecture Notes in Computer Science, January 2022) 127-137

 [ISSN 2581-5369]

Finally, I would conclude, bringing privacy as a first priority in the regulatory framework under the European GDPR and the India's DPDP Act with the respective technological innovations, will balance the technology and individual rights in the digital world.

*****

 [ISSN 2581-5369]