INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

LEGAL FRAMEWORK GOVERNING AI AND DATA PROTECTION

AUTHOR – ANSA ELCY ALEX, STUDENT AT AMITY LAW SCHOOL

BEST CITATION - ANSA ELCY ALEX, LEGAL FRAMEWORK GOVERNING AI AND DATA PROTECTION, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (5) OF 2025, PG. 598-604, APIS – 3920 – 0001 & ISSN - 2583-2344

ABSTRACT

Digital Personal Data Protection Act (DPDP Act): A New Era for DataProtection in India
The DPDP Act (Digital Personality Personal Data Protection), 2023,represents an important step in regul ating data protection in the country.The aim is to protect individual personal data and at the same ti me,ensuring that advances in businesses and technological developments,including artificial intellige nce (AI), can thrive responsibly. In contrast tothe European Union'

General Data Protection Ordinance (GDPR), whichincludes detailed guidelines for AIrelated data proce ssing, the DPDP Actis not explicitly mentioned. However, principles and obligations apply toAIcontrolle d data processing, which presents important legal andregulatory challenges.In 2022, the Indian gover nment introduced the Digital Personal DataProtection Act (DPDP Act), a comprehensive law to protect the personaldata of Indian citizens. The law is a major change in India's approach todata protection, h ighlighting the need for transparency, accountabilityand user consent[1169]The DPDP Act determines sev eral important provisions that must becompliant with the organization that processes personal data. TheseincludeMemos and Approvals: Organizations must clearly and accurately notifyyou of a clear a nd accurate notice of the collection and use of personaldata and obtain consent before processing s uch data.[1170]

Minimizing Data: Organizations simply collect and process personal datanecessary for the purposes specified in the communication.[1171]–

Data Protection according to Draft and Standard Settings:Organizations must implement data protec tion principles and protectionmeasures throughout the lifecycle of their personal data and ensure th atthe standard settings for products and services are privacy.[1172]

[1169] Digital personal data protection act , 2022 (india)
[1170] Digital personal data protection act , 2022 (india)section 5
[1171] Digital personal data protection act , 2022 (india)section 6
[1172] Digital personal data protection act , 2022 (india)section 7

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

1.1 KEY PRINCIPLES OF THE DPDP ACT AND ITS IMPACT ON AI

The DPDP Act is based on the fundamental princ iples of data protection,accountability and trans parency that directly impact AI applications.So me of the key aspects include:Consulting based data processing: The DPDP Act provides t hat datacarriers (the organizations that collet a nd process personal data) mustobtain consent from individuals (data managers) before proce ssing data.Those who rely on AI systems, partic ularly machine learning modelstrained on huge data records, face the challenge of obtaining ex plicitconsent, especially when data is used for p urposes beyond theindividual's initial understan ding.[1173] However, DPDP enforces the desiredrestri ctions. This means that data can only be used f or the specificpurposes that were collected. This could prevent AI developers from resilient data for innovation and creating friction between dat a protectionlaws and AI research.[1174] AIcontrolled companies, particularly those insectors such as healthcare, banking and social media, can be e xposed tolower obligations and stricter complia nce, including data testing and riskreviewsAI ap plications, particularly those using automated d ecisionmaking, must address these requiremen ts.[1175] For example, AIbased creditratings or AI fac ial recognition systems should ensure that indivi duals canquestion themselves about their impa ct. Indian AI startups and multinationl technolo gy companiescould face preliminary problems. ApproachtoAIThe DPDP approach also addresse s the use of artificial intelligence (AI) inthe proce ssing of personal data. The law recognizes the p otential benefitsof AI, but also recognizes risks a ssociated with its use, such as distortion,discrimi nation, and lack of transparency. Organizations need to ensureAI systems are transparent and c an receive clear and accurateinformation abou t their use of AI in the processing of personal dat a. [1176]The law provides for penalties for noncomp liance, including a fine of upto 'crores (approxim ately $6.7 million) or a company's company of2 %. The focus of the law on transparency, accoun tability and userconsent determines new stand ards for data protection in India. Hisapproach to AI recognizes the potential benefits of this tech nology, and atthe same time recognizes the risk s associated with its use.[1177]AI is carefully accept ed. The DPDP Law approach as AI continues totr ansform industry, revolutionizes our lives and w ays of working,documenting the need for a nua nced approach to DPDP law. The AI,DPDP Act req uires companies to assess their effectiveness b efore usingAI systems and processes personal d ata. These reviews should identifyand evaluate t he potential risks and consequences of AI use, in cluding therisk of distortion, discrimination and damage to people. decisionmaking. The three o rganizations should ensure that the AI systemprovides clear and accurate information about the data used for training,the algorithms used, and the decisions determined. This transp arency isimportant to build trust in AI systems a nd to help individuals understandhow personal data is used. Make decisions that have a major i mpact on the individual.[1178]

1.2 OVERVIEW OF GDPR AND ITS IMPLICATION FOR AI

The General Data Protection Ordinance (GDPR), i ssued by the EuropeanUnion in 2018, is generally considered to be one of the mostcomprehensiv e data protection laws in the world. It has been developedto protect the personal data and priv acy of people in the digital world.This regulation applies to all organizations that process person al data fromEU residents, regardless of where th e organization is based.[1179] GDPR aims toenable people with stronger control over their personal information bydetermining strict guidelines for data collection, storage and processing. Organizations must obtain the individual's express consent before processing the data and must clearly communicate how the data is used. Furthermore, the rules emphasize data

[1173] Digital Personal Data Protection Act, 2023, Section 6 (Consent Framework).
[1174] DPDP Act, 2023, Section 4 (Purpose Limitation).
[1175] DPDP Act, 2023, Section 10 (Significant Data Fiduciary Obligations).
[1176] Digital Personal Data Protection Act, 2022 (India), Section 15
[1177] Digital Personal Data Protection Act, 2022 (India), Section 16
[1178] Digital Personal Data Protection Act, 2022 (India), Section 15-19
[1179](GDPR Summary) https://www.gdprsummary.com/gdpr-summary/

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 5 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

minimization. This means that you should only collect data that is needed for a particular purpose .These principles are particularly relevant in the context of AI where large amounts of data are often processed to train algorithms. One of the most important effects of GDPR on AI is its impact on automated decision making and profiling. Article 22 of the GDPR gives an individual the right not to be determined solely by automatic processing and includes
profiling, as it requires that the algorithm betran sparent, explainable and unbiased. For AI devel opers, this means thatdata protection and secu rity are considered at every stage of the AI lifecy cle, from data collection to algorithm supply. [1180] This approach not onlyimproves compliance, b ut also provides trust with user . These rightsallo w individuals to control their data and take into account theorganization. Questions about the assurance of these rights are raisedin the case of AI systems, especially when it involves compl ex algorithmsand large data sets. By promoting ethical data practice and transparency,regulati on is not only effective, but also encourages the development oftrustworthy AI systems. Organiz ations prioritize GDPR [1181]

1.2.1 Principles of AI and GDPR:

The General Data Protection Regulation (GDPR) rests on key tenets encompassing lawfulness, fairness, and transparency, as well as purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability. These principles are designed to guarantee the protection of individual rights concerning the handling of their personal data. However, artificial intelligence (AI) applications, especially those utilizing machine learning, predictive analytics, and facial recognition, face significant hurdles in adhering to these principles. A particular challenge arises from the tendency of AI systems to gather and process data for unforeseen purposes, often conflicting with the principles of purpose limitation and data minimization. .[1182]

1.2.1 Exploring Automated Decision Making and the Right to Explanation

One of the most discussed aspects of GDPR rela ted to KI is Article 22,which grants individuals the right to make automated decisions, includingp rofiles, if such decisions have a legal or significa nt effect. [1183]This meansthat AIbased credit ratin gs, configuration algorithms, or facialrecognitio n systems must include human supervision or clearjustification. The KI model, especially DeepL earn Systems, acts as a"black box", making it dif ficult to give wise explanations about decisions. This creates legal uncertainty and practical cha llenges for AI businesses.[1184]

1.2.2 The right to participate and compatibility

GDPR grants several rights via personal data. T hese rights represent thechallenges of AIcontroll ed applications, especially for those using bigd ata analytics. For example, AI systems trained wi th personal data may bedifficult to implement t he "right to forget" because deleting the dataus ed in training may not completely remove the i mpact on the AI model(Article 17). Furthermore, t he right to data portability (Article 20) requirest hat AI systems provide individual in a structure d form. This can bedifficult when AI is coagulate d and converted in complex[1185]

1.2.3 The fairness and discrimination of AI

systems can be increased byinheriting existing distortions in training data. The GDPR emphasize s fairprocessing and prohibits discrimination ba sed on sensitive data such asbreed, gender, an d political opinions (Article 9). This means that A Idevelopers need to ensure that their algorithms do not achieve unfair orbiased results. However , ensuring AI fairness is technically complicated. This is because distortions can be embedded d eep in the data records,making them difficult to delete. Regulators are increasingly needingalgo rithm audits and fairness review to mitigate the

[1180] (the impact of GDPR in artificial intelligence) https://securiti.ai/impact-of-the-gdpr-on-artificial-intelligence/
[1181] (The impact of GDPR ON AI) https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU%282020%29641530
[1182] GDPR, Article 6 (Lawfulness of Processing).
[1183] GDPR, Article 22 (Automated Decision-Making and Profiling).
[1184] GDPR, Articles 15-21 (Data Subject Rights).
[1185] GDPR, Article 20 (Right to Data Portability)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 5 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

se risks.[1186]

1.2.4. Data Security and AI Risks

In AI systems that process personal and sensitiv e data, strict safetyrequirements of the GDPR (A rticle 32,34) are involved. AI applicationsneed to conduct strong encryption, anonymization and r isk reviews toprevent data injuries, particularly i n healthcare, financial and lawenforcement aut horities. Furthermore, GDPR privacy requires desi gnand default (Article 25) (Article 25), and the KI system can integrate dataprotection measur ements at all stages of development. This is ach allenge for businesses looking to coordinate inn ovation withcompliance.

1.2.5 Cross-border data transmission and globalization

Many AI companies are working on global and p rocess data from users inseveral urisdictions. Th e GDPR restricts the transmission of crossborder data to countries that do not have appropriate data protectionlaws (Articles (40-50)
This affects AI companies that train modelsusin g international data records or rely on cloudbas ed AI services.Companies must obtain legal me chanisms such as SCC (ContractClauses) [1187]Bi nding Enterprise Rules (BCRs) to comply with th e GDPRdata transfer rules.

1.2.5. GDPR

The future of AI regulation within the framework of the GDPR forms astrong basis for AI governm ents, but AI challenges such as Deeppake,gener ative AI, and autonomous decisionmaking do n ot posecompletely. The EU is working on AI laws that complement the GDPR bydetermining clear rules for highrisk AI applications. Future KI regul ationswill introduce stricter requirements for alg orithm transparency,accountability and fairness , allowing the design of legal environmentsfor th e processing of AI-controlled data.[1188]

1.3 KEY PRINCIPLE OF GDPR AND DPDP ACT IN AI REGULATION

General Data Protection Ordinance (GDPR) and the Digital PersonalData Protection Act 2023 (DP DP Act) represent two importantframework con ditions in the field of data protection. The GDPR i s aglobal benchmark for data protection, but th e DPDP Act reflects India'sTaylorMade approach to protecting personal data in socioeconomicco ntexts. Together, they provide valuable insight in to responsible AIregulation. The GDPR regulation s stipulate that personal data must beprocesse d legally and fairly, and provide clear communi cation aboutindividuals about how they use it. Si milarly, it is a DPDP Act consentbased processin g, requiring individual explicit and informed con sentbefore data is processed. For AI systems, th is means that data recordingand use is transpa rent, ethically welldiscovered, and encourages t rustamong users.Another general principle is Mi nimizing the data The GDPR requirescompanies to collect only the data needed for a particular purpose, andthe DPDP Act enforces similar restri ctions to prevent excessive datacollection. This principle is particularly relevant to AI where larg e datarecords are often used to train algorithms . By adhering to dataminimization, businesses c an reduce the risk of abuse and improvecompli ance. The GDPR is responsible for ensuring com pliance with thatprinciple, but the DPDP Act refer s to the "datalath" and organizationsresponsible for protecting personal data.[1189] For AI developer s, this meansthat robust governance mechanis ms are implemented and regular auditsare con ducted to ensure ethical practices. Article 22 gr ants an individualthe right not to make a decisi on based solely on automated processing ifsuc h a decision has a significant effect. Although th e DPDP Act does notexplicitly relate to automate d decisionmaking, its focus on transparencyand accountability indirectly supports ethical AI pra ctices. Thisunderscores the need for an explana tory AI system that can justify userdecisions. The GDPR requires businesses to integrate data pro tectionmeasures into their systems from the sta

[1186] GDPR, Article 9 (Processing of Special Categories of Personal Data).
[1187] GDPR, Articles 25, 32-34 (Security and Privacy by Design).
[1188] European Commission, Proposal for the AI Act (2021)
[1189] (Article what are the 7 principle of GDPR) https://www.gdpreu.org/7-main-data-protection-principles-under-gdpr/

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 5 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

rt. For AI, this means that dataprotection and se curity features are included in the algorithm, en suringcompliance with the entire AI lifecycle. Wh ile the GDPR sets a globalstandard, the DPDP m ethod provides a localized perspective thataddr esses India's unique challenges. Together they u nderscore theimportance of installing technolo gical advances with privacy andaccountability, paving the way for a safe, integrated digital futu re.[1190]

1.4 EXTRA TERRRITORIAL APPLICATION AND CROSS BORDER DATA TRANSFER REGULATION

In our interconnected world, data transcends geographical limitations, effortlessly traversing international lines through various digital channels such as cloud platforms, email systems, mobile applications, and online resources. However, the laws dictating data governance are confined within national territories, creating a discrepancy. To address this disparity, numerous legal systems have broadened their scope to encompass data processing activities occurring outside their national perimeters, a principle referred to as extraterritorial application Concurrently, regulations concerning cross-border data transfers have become paramount in safeguarding personal information, ensuring its protection even after it crosses the originating country's border. These two legal principles hold particular importance within the realm of Artificial Intelligence (AI), where AI models are frequently developed using extensive data collections sourced from global users. This section will delve into the implications of extraterritorial application and cross-border transfer regulations for AI developers and organizations involved in managing personal data. Extraterritoriality allows a country's laws to be applied beyond its geographical boundaries. In data protection, this means that organizations based outside a country must still adhere to its privacy laws if they process the data of its residents .For example, a US-based AI company providing services to Indian users is obligated to comply with India's data protection laws, even without a physical presence in India.[1191]Prominent examples of extraterritorial application in data protection include:

- General Data Protection Regulation (GDPR):Article 3 extends the GDPR's reach to data controllers and processors located outside the EU if they offer goods or services to, or monitor the behaviour of, individuals within the EU[1192]. Like the DPDP Act, the GDPR also extends its reach beyond its borders by regulating entities that process the data of EU residents, even if those entities are located outside the EU.
- Section 3(e) of India's Digital Personal Data Protection Act (DPDP Act), 2023, extends the Act's jurisdiction beyond India's borders, stipulating that it applies to the processing of personal data related to offering goods or services to individuals within India, regardless of where the processing occurs. This means that even foreign entities that process data in connection with offering goods or services to individuals in India are subject to the DPDP Act's provisions.[1193] The California Consumer Privacy Act (CCPA) applies to businesses that collect data from California residents, irrespective of whether the business is physically located within California.[1194]

The fragmented nature of international data laws necessitates a commitment to universal protection of personal data, regardless of the processing location. Organizations developing and deploying AI models cannot use geographical

[1190] (Role of AI in DPDP act transforming data privacy in india) https://corridalegal.com/role-of-ai-in-dpdp-act/

[1191] Kuner, Christopher (2015). Extraterritoriality and regulation of international data transfers in EU data protection law. *International Data Privacy Law*, 5(4), 235-245https://doi.org/10.1093/idpl/ipv019 last visited on 13/2/2025

[1192] GDPR Article 3 – Territorial Scope.

[1193] DPDP Act 2023, Section 3(e) – Application of the Act to processing in connection with offering goods or services to data principals in India

[1194] California Consumer Privacy Act (CCPA), Section 1798.140(c)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

distance to evade accountability. This is crucial because AI models trained on global data must adhere to a complex web of legal requirements.[1195]

1.4.1 Cross-border data transfer regulations.

Which is designed to maintain a consistent level of privacy protection for personal data, even when it is transferred internationally. These regulations are of paramount importance for AI systems, which often rely on cloud infrastructure deployed across various geographic regions[1196].

1.4.2 GDPR's Approach to Cross -Border Transfer.

The GDPR significantly restricts the transfer of personal data outside the EU/EEA, permitting such transfers only under specific circumstances: first, if the European Commission has recognized the destination country as providing an adequate level of data protection[1197]; second, if appropriate safeguards are implemented, such as Standard Contractual Clauses or Binding Corporate Rules; or third, if the transfer is justified by a specific derogation, for instance, explicit user consent or the necessity for fulfilling a contract. To illustrate, if an AI analytics platform located in India processes data of EU residents, it must rely on Standard Contractual Clauses unless the EU Commission grants India an adequacy decision[1198].

1.5 INDIA'S APPROACH UNDER ACT , 2023

India's Data Protection Approach Under the DPDP Act, 2023:

The Digital Personal Data Protection (DPDP) Act, 2023 governs international data transfers, granting the Central Government the power to restrict cross-border data flow via notifications, particularly to countries deemed to lack "adequate protection."

Key Points:

- The Act does not impose a complete ban on international data transfers; however, the government retains the authority to create blacklists or require approvals.
- Data fiduciaries are responsible for ensuring that international data processors adhere to equivalent data protection standards.
- The Indian legal framework prioritizes governmental oversight of data destinations over individual company security measures.[1199]

Sector Specific and Bilateral Consideration Beyond national legal frameworks:

- Specific industries, such as finance and healthcare, are subject to more stringent export control regulations regarding sensitive information.
- Nations might establish bilateral or multilateral accords, such as the EU-U.S. Data Privacy Framework, to support secure and reliable data transfers[1200]

Implication for AI Developers and Organization

For AI Developers and Organizations: Navigating the Complexities of Global AI Regulation

The interwoven nature of extraterritorial application and data transfer restrictions creates significant compliance obligations for AI companies with international operations.

Core Challenges:

- Reconciling disparate legal frameworks (e.g., aligning GDPR with the Indian DPDP Act).

[1195] Wu, Weiyue, and Liu, Shaoshan (2023). A Comprehensive Review and Systematic Analysis of Artificial Intelligence Regulation Policies. arXivhttps://doi.org/10.48550/ARXIV.2307.12218 last visited on 10/02/2000

[1196] Weber, R. H. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, 3(2), 117-130https://doi.org/10.1093/idpl/ipt001 last visited on 10/02/2000

[1197] Phillips, Mark (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human Genetics*, 137(8), 575-582https://doi.org/10.1007/s00439-018-1919-7 last visited on 10/02/2025

[1198] GDPR Chapter V – Transfers of personal data to third countries or international organisations

[1199] DPDP Act 2023, Section 16 – Transfer of personal data outside India

[1200] European Commission (2023). Adequacy decisions and international data flows – EU-U.S. Data Privacy Framework

- Integrating region-specific privacy mechanisms within AI systems.
- Enforcing data localization mandates for sensitive data types like biometric or financial information.
- Developing thorough Data Processing Agreements (DPAs) and transfer impact assessments.

Illustrative Scenario: Consider a facial recognition firm processing data of Indian citizens but utilizing servers in Singapore; the company must ensure Singapore's data protection standards are on par with India's, or risk legal repercussions under Indian law.

Recommended Compliance Approaches:

- Conduct comprehensive data flow mapping to pinpoint international data transfers.
- Employ modular AI designs to isolate sensitive data processing within specific regions.
- Leverage privacy-enhancing technologies such as encryption and federated learning.
- Maintain continuous monitoring of government announcements and legal shifts across relevant jurisdictions.
- Meta (facebook) and GDPR :Due to concerns regarding data transfers from the EU to the US, Meta encountered legal obstacles and substantial fines under GDPR, ultimately necessitating the storage of European user data on servers within the EU.[1201]
- Tik Tok in India :Citing privacy issues and geopolitical factors, India prohibited TikTok and numerous other applications, highlighting the impact of data localization and sovereignty on AI governance.[1202]

[1201] Court of Justice of the European Union, Schrems II Case (C-311/18) – Invalidation of the EU-U.S. Privacy Shield
[1202] Press Information Bureau, Government of India (2020). Ban on Chinese apps over data security concerns