Page 1091 - 1116 **DOI:** *https://doij.org/10.10000/IJLMH.1111619*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Jurisdictional Overlaps between the IT Act, 2000 and the DPDP Act, 2023 against International Standards

ALINA HUSAIN[1]

ABSTRACT

The introduction of the Digital Personal Data Protection Act, 2023 (DPDP Act) is a major change in India's data protection framework but, at the same time, it poses complicated questions about the jurisdiction in relation to the already existing Information Technology Act, 2000 (IT Act). This study determines the statutory intersections between the two regimes by examining overlapping provisions, adjudicatory mechanisms, and enforcement competencies. It explores how these overlaps can cause regulatory uncertainty, compliance burden, and inconsistent accountability in data governance. The study, using a comparative lens, considers India's dual-framework issues in light of international standards such as the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA) of the United States.

Using doctrinal and comparative legal methodologies, the paper outlines normative and institutional gaps in India's data protection framework and suggests the harmonization of strategies to improve legal coherence, regulatory coordination, and international compliance alignment.

Keywords: *Data Protection, Jurisdiction, Information Technology Act, Digital Personal Data Protection, Overlapping provisions, Enforcement, Accountability, Data Governance, International Standards*

I. INTRODUCTION

Jurisdictional overlaps have become increasingly important in India's data protection regime since the Digital Personal Data Protection (DPDP) Act, 2023[2] was recently passed. This new law is replacing the previous framework of the Information Technology (IT) Act, 2000[3], specifically the now-omitted Section 43A[4], which previously governed sensitive personal data through the SPDI Rules, 2011[5]. The DPDP Act created the Data Protection Board (DPB), a

[1] Author is a Student at Jamia Millia Islamia, Delhi, India.
[2] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[3] Information Technology Act, 2000 (Act 21 of 2000).
[4] Information Technology Act, 2000 (Act 21 of 2000), s. 43.
[5] Information Technology (SPDI) Rules, 2011 (under the IT Act, 2000).

 [ISSN 2581-5369]

specialised adjudicatory body, to enforce and impose sanctions under the new, independent, all-encompassing data protection regime that acknowledges people's rights over their digital personal data.[6]

The DPDP Act clearly states that its provisions are "in addition to and not in derogation of any other law in force"[7], highlighting a complex and interconnected regulatory framework that connects data protection to cybersecurity, consumer protection, competition law, and sectoral regulations. This is significant in consideration to the importance of jurisdictional overlaps. For example, the newly established DPB's authority under the DPDP Act is in conflict with the IT Act's strong adjudicatory role of the Adjudicating Officer, who is legally empowered to handle violations and disputes. This raises critical concerns regarding the regulatory clarity and power balance. A critical domain of such overlap includes the regulation of data breaches and unauthorized data access. While the IT Act criminalizes unauthorized access and manipulation of computer systems and data under the provision contained in Section 43, the DPDP Act emphasizes consent as a core principle for lawful data processing. The legal interplay between “permission” under the IT Act and “consent” under the DPDP Act remains unresolved, in turn, creating potential jurisdictional ambiguity in its enforcement.[8]

The regulation of data breaches and unauthorised access is a crucial area in this context. The DPDP Act highlights consent as a fundamental tenet for legitimate data processing, whereas upon further interpretation, Section 43 of the IT Act makes access to and alteration of computer systems and data illegal. Eventually there turns out to be jurisdictional ambiguity in enforcement due to the unresolved legal interaction between "permission" under the IT Act and "consent" under the DPDP Act. Consequently, the significance of these jurisdictional overlaps lies in the need for a proper legislative and institutional harmonisation to make sure effective data governance in the rapidly evolving digital ecosystem. A critical clarity in roles, procedural coordination, and alignment with international standards is extremely pivotal to safeguard data rights and foster trust in the data economy.[9]

II. THE EVOLUTION OF DATA PROTECTION IN INDIA- FROM THE IT ACT, 2000 TO DPDP ACT, 2023

Data protection in India has progressed from the basic regulatory provisions in the Information

[6] Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 18 (establishing the Data Protection Board).
[7] Information Technology Act, 2000 (Act 21 of 2000), s. 38.
[8] Srishti Kumar, ‘Exploring jurisdictional overlap in India’s data protection landscape’ (2023) *Bar and Bench*, https://www.barandbench.com/columns/exploring-jurisdictional-overlap-in-indias-data-protection-landscape.
[9] Taxmann, ‘DPDP Act vs IT Act – Shifting India’s Data-protection Paradigm’ (2025) *Taxmann*, https://www.taxmann.com/post/blog/dpdp-act-vs-it-act.

 [ISSN 2581-5369]

Technology Act, 2000, to the comprehensive regime of the Digital Personal Data Protection Act, 2023. The IT Act, 2000 was after its enactment, supplemented by the SPDI, or the (Sensitive Personal Data or Information) Rules, 2011.[10] An analytical overview of the IT Act helps understand its position as India's first legal regime for digital governance, providing limited privacy and data protection provisions. Sections 43A and 72A hold prominence in this regard. Section 43A imposed liability on body corporates for negligent handling of sensitive personal data and including the kind of data related to financial, medical, and other prescribed categories leading to compensation claims for wrongful loss.[11] Section 72A criminalized intentional and unlawful disclosure of personal information acquired under contractual terms, thus holding violators liable for imprisonment and fines.[12] The SDPI Rules, 2011 defined the constituents of personal data and prescribed reasonable security practices and consent requirements for handling such intricate information. This framework suffered from limited scope and vague definitions with inconsistent enforcement. A lack of explicit individual rights and a specialized enforcement authority added to the need for a transition to the Digital Data Protection Act, 2023.

This growing demand for a robust data protection scheme led to the enactment of the Digital Data Protection Act, 2023.[13] The act provides for a modernised statutory regime for personal data in the digital form and repealed Section 43A of the Information Technology Act, 2000. It also replaced the previous SPDI Rules and enabled a full-fledged structure centred around areas like transparency, individual rights, accountability, and enforcement. The new and efficient features of the DPDP Act include clear definitions of personal and digital personal data, strict requirements for a free, informed, and unambiguous consent prior to any type of data processing, rights for data principles, taking into consideration access, correction, erasure, grievance redressal, and several nomination rights. There are provisions for mandatory notice protocols, stringent security safeguards, and the periodic data protection impact assessments for various data fiduciaries.[14]

The DPDP Act has suggested the creation of the Data Protection Board of India for the

[10] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) dated April 11, 2011, published in the *Gazette of India, Extraordinary, Part II, Section 3, Sub-section (i).*

[11] Information Technology Act, § 43A (2000).

[12] Information Technology Act, § 72A (2000).

[13] The Digital Personal Data Protection Act, No. 22 of 2023.

[14] Taxmann, 'DPDP Act vs IT Act – Shifting India's Data-protection Paradigm' (2025) *Taxmann*, https://www.taxmann.com/post/blog/dpdp-act-vs-it-act.

 [ISSN 2581-5369]

oversight, penalization, and dispute resolution.[15] This in turn enables specialised adjudication by establishing a proper and independent, expert-driven authority highly focused on privacy disputes and their oversight. The members constitute those with special knowledge and practical experience in law, data governance, technology, and administration. Disputes and breaches involving personal data are deemed to be adjudicated by those with sector-specific expertise rather than normal tribunals, for that matter.[16]

There are heavy penalties for security breaches and the failure to comply with such safeguards leads up to a fine of almost 250 crores, including significant breaches.[17] The penalty is aimed at data fiduciaries including organisations and entities handling personal data. It tends to reflect the crucial importance of data security in the digital privacy regime. The maximum penalty for failure is such to enable the implementation of reasonable security safeguards that tend to prevent personal data breaches. Lapses in cybersecurity measures, lax controls, and the inadequate protections that expose data to unauthorised access or leaks are included. Failure to notify the related offenses to the Board and the affected ones can lead to a fine up to 200 crores, if correctly specified. Mishandling children's data and breaches by significant data fiduciaries tend to also have higher compliance obligations. The amount takes into significant consideration the nature, gravity, duration, impact, the sensitivity of compromised data and the extent of non-compliance and negligence. The fines act as a strong deterrent mechanism against negligent or malicious data practices to incentivise stringent security protocols, monitoring, and rapid breach reporting.[18]

India's approach to such a data protection regime has evolved from various fragmented and regulatory measures under the IT Act and the rules therein for a unified and a rights-based approach through the DPDP Act. This marks a fundamental shift in the country's digital landscape and in making the country's digital regulatory ecosystem. There has been a paradigm shift in the digital governance landscape in this manner. A replacement of sectoral and reactive compliance obligations with a horizontal, principle-driven regime that tends to prioritize aspects such as individual consent, data minimization, purpose limitation, and accountability, is evident through this transition. By establishing the Data Protection Board, the DPDP has been successful in aligning India's framework with the recent global frameworks like the GDPR, while retaining the sovereignty-aligned flexibilities including the exemptions for state functions

[15] Digital Personal Data Protection Act, § 18 (2023).
[16] Srishti Kumar, 'Exploring jurisdictional overlap in India's data protection landscape' (2023) *Bar and Bench*
[17] Digital Personal Data Protection Act, The Schedule, Item 1 (2023).
[18] King Stubb & Kasiva, 'Penalties and Adjudication under the DPDP Act, 2023: Powers of the Data Protection Board and Quantum of Fines' (2025) *King Stubb & Kasiva*

 [ISSN 2581-5369]

and judicial enforcement mechanisms.[19]

There are separate provisions for children's rights concerning data privacy, mandating data breach notifications and for empowering individuals with rights to access, correction, erasure, and grievance redressal. All this has led to a citizen-centric digital ecosystem. The transition sets the tone for India to be a responsible global digital player and to foster innovation with a transparent, accountable, and a secure governance architecture in the digital economy and legal arena.[20]

III. JURISDICTIONAL OVERLAPS

The jurisdictional frameworks under the DPDP Act, 2023 shares several foundational and basic principles with the leading international models, especially the ones including the EU General Data Protection Regulation, the California Consumer Privacy Act, and the APAC frameworks. There is still divergence in distinct procedural and substantive areas.[21]

Similarities between India's approach include the consent focused and rights- based approach in the GDPR, CCPA and the DPDP Act. India's framework mainly focuses on privacy rights, requiring the clear user consent and providing access to correct and erase data and the related information. There is extraterritorial application and scope that is found to be crucial. There are foreign entities that process in-scope personal data, applying to businesses that offer goods/services to data principles in India and the relevant entities in different jurisdictions. With regards to accountability and penalties, each regimes established explicit obligations for non-compliance. There is DPDP management by a centralised Data Protection Board that resembles the GDPR-style regulatory oversight. There is difference, though in independence and the related mechanisms.[22]

With reference to the APAC countries including Singapore PDPA, Australia Privacy Act, and Japan APPI, the mechanisms broadly align in areas like transparency, purpose limitation, and breach notification. There is variation in enforcement and cross-border transfer rules that are studied as a separate point in various legal researches. Such frameworks are more sectoral and

[19] Press Information Bureau (PIB), Government of India, 'Government notifies DPDP Rules to empower citizens and protect privacy' (2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014.
[20] Digital Personal Data Protection Act, §§ 8(6), 9, 12-16 (2023).
[21] Consent, 'What is the difference between DPDP Act and GDPR?' (2023) *Consent*, https://www.consent.in/blog/dpdp-vs-gdpr.
[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1., Cal. Civ. Code § 1798.100 et seq. (West 2018).

region-specific, while DPDP Act focuses more on government oversight and data localisation, making multinational alignment more complex and sophisticated.[23]

The key differences and distinct approaches have been included in the table provided below-

Feature	India DPDP Act	GDPR	CCPA/APAC Frameworks
Regulator Independence	Appointed by central government; limited autonomy	Independent public authorities	Independent/State agencies
Sensitive vs Personal Data	No distinction; all personal data treated uniformly	Sensitive data gets additional protection	CCPA distinguishes "sensitive"
Government Exemptions	Broad exemptions for sovereignty, law enforcement	Strict necessity, proportionality for exemptions	Varies; CCPA/CPRA less broad
Cross-Border Data Transfers	Government lists banned countries; process flexible, not standardized	SCCs, BCRs, adequacy decisions — business-driven	APAC regimes highly fragmented
Private Right of Action	No private right for data subjects	Provided for individuals	Limited: CCPA allows opt-out
Data Localization	Strong localization emphasis; periodic review by government	Limited localization; adequacy-based	APAC: e.g., China, Indonesia
Child Data Protection	18+ threshold, uniform rules, extra parental consent	Under 16, more granular rules	APAC approaches vary

Overlaps in jurisdictional scenarios commonly arise in breach notification and redress. Indian authorities tend to mandate notifications and parallel investigations by consumer or sectoral regulators in areas like telecom, health and business. This excludes notions like the GDPR

[23] IAPP, 'Global Privacy Law and DPA Directory' (2025) *International Association of Privacy Professionals*, https://iapp.org/resources/global-privacy-directory/.

DPAs or the U.S. state Attorney Generals. There are overlaps in consent and processing standards. DPDP's stringent and uniformly applied consent regime diverges from GDPR/CCPA's requirements. This is turn, generates uncertainty where more than one standard applies to the scenario and where local standards demand compliance layering.[24]

IV. ENHANCED COMPLIANCE CHALLENGES AND STRATEGIES

There is a complex compliance landscape in India with regards to multinational companies. This goes beyond the simply translating global privacy frameworks. The DPDP Act tends to treat all personal data uniformly and requires MNCs to recalibrate internal data classification and the relevant risk assessment protocols. Sensitive data distinction causes ambiguity for sectors including healthcare, finance, or cloud services.

DPDP mandates user notices in various Indian languages and simple consent-first mechanisms. There is requirement for companies to deploy regionally tailored interfaces. Grievance redressal mechanisms and withdrawal of consent have to be accessible and user-friendly. This is in stark contrast to the more flexible opt-out mechanisms and regimes under the CCPA and the nuanced consent hierarchy under GDPR. There are certain statutory exemptions as well that allow broad governmental and laws enforcement exemptions. MNCs that are accustomed to prescriptive and narrow GDPR/CCPA carve outs tend to face compliance uncertainties and more so when the government seeks access or issues directives for data localisation.[25]

In contrast to the GDPR, which provides regulatory clarity for cross-border operations through the lead authority principle, India's sovereignty-driven, centralised Data Protection Board may lead to interpretive ambiguity when its duties overlap with those of sectoral regulators or legacy IT Act regimes. MNCs or large domestic businesses above certain thresholds (e.g., user volume, nature of processing, or risk) face advanced compliance: appointment of a resident Data Protection Officer, periodic Data Protection Impact Assessments, independent audits, and enhanced internal controls. The standards for SDFs resemble GDPR's "high-risk processing" triggers but are accompanied by direct government oversight rather than independent or sectoral authorities.[26]

---

[24] Ardent Privacy, 'GDPR Vs India's DPDPA: Key Differences And Compliance Implications' (2025) *Ardent Privacy.*

[25] Zou Global Services, 'Decoding India's DPDP Act: A Privacy Leader's Perspective' (2025) *Zou Global Services*. See also King Stubb & Kasiva, 'Consent Framework under the Digital Personal Data Protection Act, 2023: Legal Requirements and Compliance Strategies' (2025) *King Stubb & Kasiva.* See also*, Latham & Watkins LLP, 'India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison' (2024) Latham & Watkins LLP.*

[26] ANI News, 'Government notifies DPDP rules to empower citizens, protect privacy' (2025) *ANI News*, https://www.aninews.in/news/business/government-notifies-dpdp-rules-to-empower-citizens-protect-

With the exception of nations where government restrictions are specifically in place (no adequacy or contractual safeguard regimes yet), DPDP permits cross-border data transfers. The domestic focus of the CCPA and the established transfer mechanisms (SCCs, BCRs) of the GDPR do not address the challenge faced by MNCs when draughting contracts: they must account for localisation requests, anticipate rapid regulatory change, and maintain alignment with international standards.[27]

Under the DPDP Act, multinational companies operating in India need a constant and proactive approach to managing risks and related problems. Instead of depending on one-time certifications or registration systems, these businesses need to appoint qualified Data Protection Officers (DPOs). They also need to keep detailed records of data processing activities and regularly audit their compliance to be ready for regulatory inquiries at any time. Thorough contractual and operational documentation is crucial. MNCs should map and document all data flows related to India, frequently update internal and third-party privacy policies, provide regular training programs, and create strong procedures for escalation and response. This will help them remain ready for audits and agile as requirements change.[28] Additionally, there is now an increased expectation of accountability from the board and leadership. Indian regulations require boards and CXOs to stay informed and participate actively in compliance briefings. They also expect top-level responsibility for any lapses in data protection. This reflects a standard that matches, and in some ways goes beyond, the accountability requirements in frameworks like the CCPA and the GDPR. This signifies a major shift toward a culture of continuous compliance and governance throughout the organization, rather than relying on static or reactive measures.[29]

V. INTERNATIONAL STANDARDS: JURISDICTIONAL CONFLICTS

Worldwide data protection norms have changed to tackle the complicated issues of the digital age, such as dealing with conflicts between jurisdictions, encouraging regulatory harmonization, and allowing secure cross-border data flows. The extraterritorial effects of contemporary data privacy laws are the main reasons for jurisdictional conflicts, as several countries may claim that they have the authority to regulate the processing of personal data. To avoid such conflicts, international standards resort to the principles of territoriality—

privacy20251114215316.

[27] Crossing Borders: Comparative Perspectives on Data Protection Laws in India, the EU, and the US' (2024) *Journal of Data and Information Privacy Research* Vol. 1, No. 2.

[28] Digital Personal Data Protection Act, §§ 8, 9(1), 10, 11 (2023); Taxmann, 'Digital Personal Data Protection (DPDP) Act 2023: Compliance Roadmap' (2024) *Taxmann.*

[29] Digital Personal Data Protection Act, § 10(2)(a) (2023); King Stubb & Kasiva, 'The Data Protection Board of India under the DPDP Act, 2023: Structure, Composition, and Adjudicatory Process' (2025) *King Stubb & Kasiva*.

determining jurisdiction on the basis of either the place where data processing takes place or the person targeted. Moreover, these norms stipulate that enforcement should be proportionate and that there should be restraint in order to prevent a legal overreach and to facilitate a good working relationship between different jurisdictions. Privacy is protected in this way together with other rights as states' sovereignty is respected.

One of the important aspects of global privacy initiatives is also regulatory harmonization. Different regulations like the European Union's General Data Protection Regulation (GDPR)[30], the Asia-Pacific Economic Cooperation (APEC) Privacy Framework[31], and the OECD Privacy Guidelines[32], together with other similar ones, encourage the implementation of shared principles such as data minimization, transparency, and respect for the rights of the individual in different territories. These standards make it easier for countries to enter into mutual recognition or adequacy agreements whereby they agree that their respective data protection frameworks are equally strong enough. Such harmonization makes it easier for multinational companies to be in compliance with the law and also encourages cooperation among regulators which is beneficial for the uniformity of privacy rights worldwide.

Cross-border data flows remain the backbone of the global economy, but they carry privacy risks that international standards seek to manage without impeding innovation. Accordingly, these standards mandate that data controllers install safeguards when they transfer personal data to data territories with different or less stringent protections. Some of these safeguards are the signing of standard contractual clauses, binding corporate rules, or making sure that the recipient countries have been granted adequacy status by the supervisory authorities. Such a measure allows data to be rifled through any border without breaching security, thus striking a balance between data utility and privacy rights.

Combined together, international data protection standards are a trade-off between privacy and the facts of a connected world by lessening jurisdictional conflicts, harmonizing regulatory approaches, and permitting trustworthy data exchanges.

VI. INDIA'S APPROACH

Global compliance and data governance frameworks will be significantly impacted by India's

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.
[31] Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (Revised 2015).
[32] Organisation for Economic Co-operation and Development, *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(2013)79 (2013).

 [ISSN 2581-5369]

approach to data protection through the Digital Personal Data Protection Act, 2023 (DPDP Act). India positions itself as a major participant in the global data economy while defending its interests by adhering to international privacy and data security standards while introducing unique regulatory features. Due to the DPDP Act's extraterritorial applicability, multinational corporations handling Indian personal data—including those without a physical presence in India—must abide by India's data protection regulations. This makes it necessary to incorporate India-specific compliance measures into their more comprehensive global data governance strategies, which will make compliance environments more complex while enhancing the strength of global data protection initiatives.[33]

India's more flexible approach to cross-border data transfers allows free data transfers to all countries except those on a government blacklist. This is different from the European Union's GDPR, which has stricter requirements for adequacy and contractual safeguards. This model seeks to balance data privacy protection with economic growth by giving businesses some regulatory certainty and operational flexibility. But this method also puts a lot of weight on government oversight, which could make it easier for some frameworks to control international data flows than others. As a result, multinational companies must use careful risk management strategies to deal with India's changing rules and regulations. This means making sure that data security and privacy rules are followed while still taking advantage of global data exchanges.[34]

India's data protection laws also emphasise the importance of openness, responsibility, and individual rights, which is in line with global data protection goals. The DPDP Act sets up new ways to improve governance structures, like the Data Protection Board, which will oversee enforcement, punish people who don't follow the rules, and settle disputes. India's model of data governance is a good example of a middle ground between strict data localisation rules and free data flows. It has an impact on international talks about how to make data protection laws more consistent. India's laws have a unique regulatory philosophy that requires ongoing conversations among international stakeholders to resolve differences, make sure that systems can work together, and encourage safe cross-border data sharing that protects privacy while promoting innovation and economic integration.[35]

---

[33] Digital Personal Data Protection Act, § 3(b) (2023); Baker McKenzie, 'Territorial Scope | India | Global Data and Cyber Handbook' (2024) *Baker McKenzie Resource Hub*.

[34] Digital Personal Data Protection Act, § 16 (2023). See also, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016... (General Data Protection Regulation), [2016] OJ L 119/1, Arts. 44-50.

[35] Digital Personal Data Protection Act, § 16 (2023); King Stubb & Kasiva, 'Cross-Border Data Transfers under the DPDP Act, 2023: Government's Power to Whitelist and Blacklist Jurisdictions' (2025) *King Stubb & Kasiva*; 'Crossing Borders: Comparative Perspectives on Data Protection Laws in India, the EU, and the US' (2024) *Journal of Data and Information Privacy Research* Vol. 1, No. 2.

 [ISSN 2581-5369]

Thus, the approach of India towards data protection has wide ramifications on the global compliance frameworks as it demands more adaptive and comprehensive data governance among multinational entities. It also contributes to the evolving international architecture of data protection by introducing an alternative model based on sovereign oversight underpinned by flexible yet accountable mechanisms for data transfers, reflecting the technological realities along with socio-political priorities.

VII. CASE ILLUSTRATIONS

Schrems Case II

Schrems II case, formally named as Data Protection Commissioner v Facebook Ireland Ltd & Maximilian Schrems (2020), is a landmark ruling by the Court of Justice of the European Union (CJEU) that greatly changed the situation of international data transfers. Besides, the Court tore down the EU-US Privacy Shield mainly because US surveillance laws did not allow the US to ensure the data were protected in a way 'essentially equivalent' to the General Data Protection Regulation (GDPR) as required by the CJEU. One of the most important factors that influenced the Court's decision was the Snowden disclosures that revealed how the US intelligence agencies accessed the private information held by US companies.[36]

In particular, the CJEU considered that US laws allowed governments' wide access to private information without, at the same time, proper judicial control and without giving enforceable rights to Union citizens. Hence, this was a clear breach of their fundamental rights under the EU Charter. The Court insisted on the use of Standard Contractual Clauses (SCCs), but at the same time it set very strict requirements that they should perform a very careful legal risk assessment in the recipient country before actually sending the data there.[37] The decision in this case basically pointed out that we live in a very precarious world where data can go only if they have secure paths, and it is very uncertain for the moment how data can be transferred between two continents, i.e., across the Atlantic. In consequence, there have been many suggestions for new agreements or, at least, for better safeguards in place. Moreover, it underscores the difficulties of trying to balance the need for national security with the need for data protection in a globally interconnected world. It also has implications for multinational corporations that have to deal with the complexity of cross-border data flows in various parts of the world.

[36] Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems (Schrems II), C-311/18, [2020] ECR I-541, [2020] 2 CMLR 10 (CJEU).
[37] Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems (Schrems II), C-311/18, [2020] ECR I-541, [2020] 2 CMLR 10 (CJEU); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016... (General Data Protection Regulation), [2016] OJ L 119/1, Arts. 46, 52.

 [ISSN 2581-5369]

Aadhar Breach

With over 1.1 billion people registered in the Unique Identification Authority of India (UIDAI) database, the Aadhaar data breach in India, which was widely publicized in early 2018, is one of the biggest exposures of personal data in modern history.[38] In contrast to a traditional cyberattack, this breach was mainly caused by systemic flaws in governance and access controls, whereby unauthorized agents sold login credentials and gained unfettered access to the personal data of almost all registered users by taking advantage of lax authentication procedures. According to investigations, this flaw was long taken advantage of by WhatsApp groups, where these login credentials were frequently exchanged for small amounts of money, thereby getting around technical security measures and making the system as a whole vulnerable.[39]

The stolen data included personally identifiable information (PII), like people's names, addresses, phone numbers, email addresses, and in some cases, biometric data like photos. UIDAI said that biometric data like fingerprints and iris scans were still safe, but the fact that demographic and identity data were available was enough to allow identity theft, financial fraud, phishing, and other bad things to happen. This breach was made worse by other breaches of government websites and state agencies that accidentally made Aadhaar-linked data public, which made the problem even bigger and worse. The crisis made it clear that centralized biometric databases are always at risk, especially when security governance is weak or not well-defined.[40]

From a regulatory point of view, this breach showed that India's data protection framework was still very new and had serious problems. It didn't have strong enforcement mechanisms or specialized adjudication bodies that could quickly respond to large-scale privacy incidents. Digital services and commerce are global, so Indian citizens' data could be processed by companies based in other countries or by companies that do business in many countries. This breach also showed how hard it is to keep up with changing international privacy standards, like the EU's GDPR.[41] It stressed the need for a clear and complete data governance system in

[38] Khaira, Rachna, 'Rs 500, 10 minutes, and you have access to billion Aadhaar details' (2018) *The Tribune*; World Economic Forum, 'The Global Risks Report 2019: 14th Edition' (2019) *WEF Global Risks Report*, 37.

[39] World Economic Forum, 'The Global Risks Report 2019: 14th Edition' (2019) *WEF Global Risks Report*, 37. *(This report highlights that the breach was due to "lax cyber security protocols," supporting the claim that the cause was governance and access control failure rather than a traditional cyberattack.)*

[40] 'The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment' (2019) *Jackson School of International Studies, University of Washington*. https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/

[41] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) dated April 11, 2011, published in the *Gazette of India...*; 'The Aadhaar

 [ISSN 2581-5369]

India that includes legal requirements, technical protections, clear accountability, and judicial oversight to keep sensitive citizen data safe. The Aadhaar breach raised serious social and political concerns about how accountable the government is for running huge digital identity systems, in addition to privacy issues. The data leak hurt people's faith in India's ambitious plans for digital identity and public service delivery. This led to calls for stricter laws and more training for government workers. It brought attention to the need to use technology to improve government functions while also making sure that it doesn't violate basic rights or create systemic weaknesses.

In conclusion, the Aadhaar data breach revealed the scope of security issues associated with centralized biometric databases as well as the pressing need for thorough data protection regulations, organized security measures, and responsible governance systems. It serves as a warning to nations creating national identity systems and emphasizes the significance of incorporating institutional, legal, and technical safeguards that are sensitive to changing cyberthreats and demands for international compliance.

Qantas Breach

The Qantas data breach in Australia, which occurred in July 2025, represents a significant cybersecurity incident affecting approximately 5.7 million customers. The Qantas third-party call centre platform became the target of hackers who gained unauthorized access to steal a large amount of customer information. The stolen information primarily included names, email addresses, frequent flyer numbers, and, for a smaller subset of records, details such as home and business addresses, birth dates, phone numbers, and meal preferences. The airline confirmed that no financial information or passport data or login information was exposed. Yet, the leaked information creates a risk for phishing schemes, identity theft, and social engineering attacks.[42]

The security breach demonstrates how third-party service providers create fundamental weaknesses when they manage essential customer information. The attackers used a vendor platform vulnerability to attack instead of targeting Qantas core systems which proves that organizations need to protect their entire supply chain network. Different organizations have started to identify supply chain vulnerabilities because of this incident which shows the need to build proper third-party risk management systems.[43]

Card: Cybersecurity Issues with India's Biometric Experiment' (2019) *Jackson School of International Studies, University of Washington*.

[42] Qantas Group, *UPDATE ON QANTAS CYBER INCIDENT: WEDNESDAY 9 JULY 2025* (July 9, 2025) Qantas Newsroom, [URL]; Cyber Management Alliance, *Qantas Data Breach: Scattered Spider Takes to the Skies?* (July 3, 2025) Cyber Management Alliance Blog.

[43] Cyber Management Alliance, *Qantas Data Breach: Scattered Spider Takes to the Skies?* (July 3, 2025) Cyber

The data breach created multiple regulatory issues that needed to be solved. Qantas had to follow Australia's Privacy Act[44] which required them to disclose data breaches to both customers and regulatory bodies while facing potential fines. However, the cross-jurisdictional nature of data — involving possibly foreign customers or suppliers — meant that other data protection regimes, such as the European GDPR or India's DPDP Act, could have relevance, depending on the affected data subjects. The management of multiple regulatory bodies across the world creates difficulties for legal accountability and enforcement because it becomes unclear which laws should apply to remediation efforts and how to properly handle rights and remedies for the vast number of customers who live outside their home country.[45]

Qantas took active steps by working with cybersecurity professionals and law enforcement, securing court injunctions to prevent further misuse or dissemination of the stolen data. Experts doubt that legal orders function as an effective tool to stop stolen information from spreading across dark web networks. The public started to criticize the airline because it failed to provide timely and enough information to its customers which proved that open communication stands as a vital element for handling data breaches. This security breach illustrates a warning to organizations worldwide because it shows how service provider ecosystems now face increasing threats from advanced cyberattacks. The situation requires organizations to maintain complete cybersecurity practices and strong legal agreements and monitoring systems for their third-party vendors and to establish systems that handle regulatory demands from multiple jurisdictions. The situation demonstrates ongoing difficulties in uniting data protection standards from various legal systems with operational requirements which requires enhanced global collaboration to create unified standards for international data protection and breach response systems.[46]

AIIMS Ransomware Attack

The All India Institute of Medical Sciences (AIIMS) in New Delhi faced a ransomware attack which started in 2022 and extended its impact until 2025. The incident stands as one of the most alarming cyber incidents in India's healthcare sector. The attack created major disruptions to hospital operations because it shut down vital digital systems which handled patient information

Management Alliance Blog.

[44] Privacy Act 1988 (Cth).

[45] Qantas Group, *UPDATE ON QANTAS CYBER INCIDENT: WEDNESDAY 9 JULY 2025* (July 9, 2025) Qantas Newsroom, [URL]; 'CROSS-BORDER DATA PRIVACY AND LEGAL SUPPORT: A SYSTEMATIC REVIEW OF INTERNATIONAL COMPLIANCE STANDARDS AND CYBER LAW PRACTICES' (2025) *American Journal of Scholarly Research and Innovation* Vol. 3, Issue 1, 31.

[46] Cyber injunctions put victims at risk, experts warn (October 27, 2025) *Information Age - ACS*. [https://ia.acs.org.au/article/2025/cyber-injunctions-put-victims-at-risk--experts-warn.html]

 [ISSN 2581-5369]

and appointment management and billing operations and laboratory results and outpatient services. The security breach exposed about 40 million patient records which included sensitive personal information of patients and healthcare staff members and blood donation data and ambulance operation details and vaccination records and caregiver contact information and staff access codes.[47]

The LockBit ransomware group executed the attack by encrypting large amounts of sensitive information before demanding a cryptocurrency payment which reached approximately Rs 200 crore (about $24.5 million).[48] AIIMS needed to switch all its operations to manual systems for an extended duration which created difficulties in patient treatment and administrative operations at one of India's largest healthcare facilities. The e-hospital system hosted on the MeghRaj national cloud platform was brought down, exposing significant vulnerabilities in India's critical healthcare infrastructure and enterprise information systems.[49]

The investigation showed that multiple cybersecurity flaws existed throughout the system because firewalls had incorrect settings and network switches remained unmonitored and employees received no proper security training and antivirus systems operated with outdated protocols. The attackers achieved full system access because of these basic security weaknesses which allowed them to launch their ransomware attack successfully. The event revealed two major problems about healthcare cybersecurity preparedness and operational security maturity which showed healthcare organizations must invest in secure systems and staff development and ongoing risk management.[50]

The breach created significant worries about the protection of sensitive health data through its effect on data confidentiality and integrity and availability which are fundamental to safeguarding personal information. The attack demonstrated that organizations must follow strict data protection regulations which include the US Health Insurance Portability and Accountability Act (HIPAA)[51] and India's Digital Personal Data Protection Act of 2023[52]. The

[47] FIR No. 250 of 2022 (Delhi Police, Intelligence Fusion and Strategic Operations Unit) (Invoking sections of the Information Technology Act, 2000, including S. 66F for Cyber Terrorism, and sections of the Indian Penal Code, 1860, including for Extortion).
[48] Srivastava, Ashish, 'AIIMS Delhi: Held to ransom by cyberattack' (2022) *The New Indian Express*, 28 Nov. 2022; 'AIIMS Ransomware Attack - Cyber Management Alliance' (July 5, 2023) *Cyber Management Alliance Blog*.
[49] FIR No. 250 of 2022 (Delhi Police, IFSO Unit) (Invoking IT Act, S. 66F, and IPC); 'TOPIC : CYBERATTACK ON CRITICAL INFORMATION (CI) INFRASTRUCTURE- A CASE STUDY OF RANSOMWARE ON AIIMS' (2023) *Lukmaan IAS Blog*.
[50] *Ibid.*
[51] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.).
[52] Digital Personal Data Protection Act, No. 22 of 2023.

 [ISSN 2581-5369]

event triggered increased policy discussions about creating specialized judicial systems and cybersecurity response systems which should become part of healthcare governance structures.[53]

The regulatory response required reporting to various agencies which included the National Informatics Centre and Indian Computer Emergency Response Team and Delhi Police and Intelligence Bureau and Central Bureau of Investigation and National Investigation Agency and Ministry of Home Affairs. The Delhi Police took legal action by filing a case which included cyber terrorism and computer-related fraud charges because the incident presented a serious threat to national security through its potential foreign involvement.[54] AIIMS ransomware attack reveals multiple security deficiencies which impact healthcare cybersecurity systems and data protection systems that exist in India. The protection of digital health systems demands a complete defence system which unites technical solutions with legal frameworks and institutional monitoring and global collaboration to fight against modern cyber threats. The attack shows public institutions which process personal data must build cyber resilience to protect privacy and security and maintain essential service operations.

VIII. PRACTICAL CHALLENGES FACED

The overlapping jurisdictions between regulatory bodies create multiple operational difficulties which emerge from conflicting legal standards and different enforcement systems and distinctive cultural perspectives about data protection. The extraterritorial scope of modern data protection laws including the European Union's GDPR and India's Digital Personal Data Protection Act (DPDP) creates major challenges for regulatory bodies. These laws establish authority through both territorial boundaries and the identification of people who live within certain areas or whose personal information gets processed anywhere in the world. The existence of multiple regulatory systems creates a complicated enforcement environment because different regulatory bodies possess conflicting responsibilities which hinders their ability to perform joint investigations and international cooperation and unified legal decision-making. The allocation of resources between regulatory bodies for mutual assistance and cross-border investigations and whistleblower management remains restricted because of existing legal frameworks and diplomatic limitations.[55]

---

[53] Digital Personal Data Protection Act, No. 22 of 2023; 'TOPIC : CYBERATTACK ON CRITICAL INFORMATION (CI) INFRASTRUCTURE- A CASE STUDY OF RANSOMWARE ON AIIMS' (2023) *Lukmaan IAS Blog*.

[54] FIR No. 250 of 2022 (Delhi Police, IFSO Unit) (Invoking IT Act, S. 66F, and IPC); 'AIIMS Cyberattack - The Aftermath' (2025) *Legal Era Magazine*.

[55] Digital Personal Data Protection Act, § 3(b) (2023); Regulation (EU) 2016/679 of the European Parliament and

Businesses face multiple challenges when they try to comply with different data protection regulations which often contradict each other. Organizations must handle different operational requirements about consent rules and data storage requirements and data transfer limitations which generate higher compliance expenses and create complex IT systems that impact service delivery operations. The absence of unified regulatory standards makes standard contractual clauses and binding corporate rules that work under one system fail to meet requirements of another system which forces businesses to create specific controls and monitoring systems for each jurisdiction. The essential cross-border data flows for technological progress and cloud computing and artificial intelligence and digital commerce operations face legal threats about data sovereignty and liability. Businesses face multiple jurisdictional reputational dangers through data breaches and enforcement actions which require continuous monitoring of changing regulatory requirements.[56]

On an individual level, overlapping jurisdictions create uncertainty and potential gaps in data subject rights and remedies. The complex nature of jurisdictional boundaries leads to uncertainty about personal rights and available legal solutions. People encounter difficulties when trying to understand their data protection laws and which organizations they can contact for violations. The overlapping jurisdictions produce uncertain legal frameworks which result in ambiguous rights for people to protect their data and obtain proper legal solutions. The existence of multiple jurisdictional systems creates uncertainty about which laws should apply to data protection matters. The conflicting rules from different jurisdictions create problems for data protection because people become unsure about their rights and legal solutions. People experience difficulties because they cannot determine which laws shield their data and how to exercise their rights for access and correction and deletion and which authority to contact when their rights get violated. The unclear jurisdictional authority between different regions creates legal challenges which make it difficult for victims to obtain swift justice through proper legal channels.[57]

The worldwide data protection system faces operational obstacles because its multiple fragmented systems operate independently. These challenges demand stronger international

of the Council of 27 April 2016... (General Data Protection Regulation), [2016] OJ L 119/1, Art. 3; 'CROSS-BORDER DATA PRIVACY AND LEGAL SUPPORT: A SYSTEMATIC REVIEW OF INTERNATIONAL COMPLIANCE STANDARDS AND CYBER LAW PRACTICES' (2025) *American Journal of Scholarly Research and Innovation* Vol. 3, Issue 1, 31.

[56] 'Global Data Privacy Compliance: Challenges and Strategies for Interoperability' (2024) *Journal of Law, Technology and Policy* Vol. 10, No. 4.

[57] 'Regulatory Fragmentation and the Erosion of Individual Data Subject Rights in Cross-Border Data Flows' (2023) *Int'l Rev. L. & Data* Vol. 5, No. 1.

 [ISSN 2581-5369]

collaboration and regulator communication and policy development. The development of legal standards that work together needs to happen alongside the creation of compatible enforcement systems and business-friendly compliance systems. The digital economy requires this comprehensive method to protect privacy rights while allowing its operations in an interconnected world.

IX. STRENGTHS AND WEAKNESSES

The Digital Personal Data Protection Act, 2023 (DPDP Act) has provided India with a new regulatory framework for data protection that is a major milestone but at the same time it has made the already existing legal jurisdictions overlapping with the Information Technology Act, 2000 (IT Act) and sectoral regulations very difficult to separate since the DPDP Act has now made it a case of unifying the strengths and weaknesses in the existing regulations.

One of the major advantages of the DPDP Act is its all-encompassing method of shielding personal data. It has established principles such as, informed consent, data minimization, and accountability and has to a certain extent, further strengthened the latter through a specialized adjudicating body—the Data Protection Board of India (DPB). The law very clearly mentions in Section 38 that it is "in addition to and not in derogation of any other law," thus conceding the complex legal environment in India where data protection overlaps with cybersecurity, consumer rights, competition law, and more. This recognition is essential for creating a regulatory atmosphere that is supportive and not combative.[58]

Nevertheless, difficulties are emphasized when there is an intersection and may be existing laws' conflicts, particularly the IT Act. The removal of Section 43A of the IT Act, which dealt with data breach compensation claims, leads to the dominance of the DPDP framework as the main referring point for data breach adjudication, but the extensive provisions of Section 43 concerning unauthorized access to computer systems still apply.[59] This gives rise to confusion in cases where data is accessed without authorization, since the criteria for "permission" under the IT Act and "consent" under the DPDP Act may not be the same. This situation of dual applicability results in a legal grey area about which jurisdiction applies—whether the adjudicating officer under the IT Act or the DPB should have the power. To make this more complex, the DPDP Act's failure to include explicit compensation rights for data principals indicates that the remedy provisions under the IT Act could still run superimposed, thus resulting in dual proceedings and overlaps.

[58] Digital Personal Data Protection Act, 2023, No. 26 of 2023, § 38.
[59] Information Technology Act, 2000, ss. 43, 43A (repealed).

 [ISSN 2581-5369]

At present, poorly developed institutional coordination and lack of clear delineation of responsibilities among the authorities are the main obstacles. The DPB's functioning, its interaction with adjudicating officers, and its cooperation with CERT-In (the Indian Computer Emergency Response Team) in cyber incidents will become evident only after operationalization and rules notification.[60] In the absence of such clarity, the parties involved in litigation and the regulators could be subject to enforcement actions that are overlapping, inconsistent, or even contradictory, which would have a negative impact on the already existing uncertainty for both businesses and individuals.

X. RECOMMENDATIONS

India's legislative scheme, from a legal perspective, aims to be in harmony with international norms at a very general level, and it is making self-intensive moves by incorporating basic data protection values to the European GDPR and other worldwide frameworks, among others. Nevertheless, there are differences in approach such as the centralization of control over cross-border data transfers which is contrary to the GDPR's decentralized adequacy determinations and contractual transfer mechanisms. This centralization might cause difficulties in compliance for multinational companies and it will also have an impact on India's global data interchange ecosystem.[61]

India's jurisdictional overlaps and regulatory clarity management can be better by implementing the following recommendations:

1. Legislative Clarity: It is necessary to amend or clarify the provisions that describe the exact jurisdiction and the remedies given by the DPDP and IT Acts when the case of the compensation and adjudicatory authority is involved, in order to reduce the cases of concurrent jurisdiction and legal uncertainties.
2. Institutional Coordination: The cooperation protocols between the Data Protection Board, adjudicating officers, CERT-In, and sectoral regulators should be improved in order to facilitate enforcement, avoid replication, and promote unified complaint redressal, e.g., through a specially created inter-agency co-ordination committee.

[60] Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025 (notified Nov 2025) (on operationalization and phased enforcement timelines of the DPB).

[61] Digital Personal Data Protection Act, 2023, s. 16; Digital Personal Data Protection Rules, 2025, Rule 15; "Cross Border Data Transfers under the DPDP Act," Leegality (July 2024); "Cross-Border Data Transfers under the DPDP Act 2023," Taxmann (May 2025); Keyur Shah, “India's New Cross-Border Data Transfer Framework,” KS & K Legal (Nov 2025).

 [ISSN 2581-5369]

3. Rules & Operational Guidelines: The detailed rules should be issued to clarify the operational aspects of conflict resolution among regulators, processes for concurrent jurisdiction, and relations with other regulatory domains such as competition and consumer law.
4. Alignment with International Standards: Over time, India can implement globally accepted methods for cross-border data transfers like adequacy determinations, standard contractual clauses, and binding corporate rules, thus making global compliance easier and creating trust among global partners.
5. Capacity Building: The training sessions should be introduced and funded for adjudicators, regulators, and businesses so as to enable them to understand the interaction of the overlapping regulatory requirements and to be able to create strong compliance models which will effectively handle multifaceted legal obligations.[62]

To sum up, the DPDP Act of India carries significant elements of advancement in the protection of personal data. However, its relationship with the already existing laws has led to complications regarding the division of powers and functioning of the authorities. It is very important to solve these problems by betterment of the law, good cooperation between institutions and compliance with the international standards in order to provide a data protection system which would be clear, convenient for the business sector and respectful of the users' rights, capable of handling the overlaps and generating confidence in the digital economy in India.

XI. CONCLUSION

The evolution of India's data protection regime, powered by the Digital Personal Data Protection Act (DPDP) 2023, is a landmark move to manage the complexity of personal data in a digitizing society. The key findings reveal that India has made a significant leap in setting up comprehensive legal standards for consent, processing, rights of data principals, and enforcement through the specialized Data Protection Board of India (DPB). Nevertheless, the regime is struggling with substantial jurisdictional overlaps with the existing laws, mainly the Information Technology Act, 2000 (IT Act), and sectoral regulations like telecommunications, financial services, and competition law. The overlapping jurisdiction creates legal ambiguity regarding the adjudicatory competence, enforcement scope, and remedies for individuals,

[62] Srishti Kumar, "Navigating Jurisdictional Intersection in India's Data Protection Regime," Dalaw.in (Mar. 23, 2021); Srishti Kumar, "Exploring Jurisdictional Overlap in India's Data Protection Framework," BarandBench.com (Sept. 27, 2023); ExpressComputer.in, "Enforcement Gaps in India's DPDP Act," (July 2025); AZB Partners, "The Digital Personal Data Protection Act Analysis," (Sept. 2023).

 [ISSN 2581-5369]

thereby making it difficult for businesses to comply and reducing regulatory certainty.

The consequences are significant. To the extent that, India's data protection system is fairly in line with the worldwide standards as it recognizes basic privacy principles and creates a separate regulatory authority. This makes India a part of the global data economy and is a suitable answer to the rising digital rights protection demands. However, the presence of parallel legal frameworks without a clear boundary between them poses the risk of repeated procedures, the inconsistency of the regulatory actions, and increase in the number of cases. Business entities experience an aggravation of their operating costs and compliance risks as they try to come to terms with these intersecting dos and don'ts, which in turn may lead to a decrease of innovation or the cross-border data flows involvement. Overlapping jurisdictions may make it difficult for individuals to obtain effective remedies, redress, and clarity regarding their rights.

Continued reform of regulations is still necessary in this case. One of the important aspects of the reform is the clarification of the relations and the resolution of conflicts between the DPDP Act and the IT Act's provisions. For example, it would be helpful to clarify the scope of Section 43 concerning unauthorized data access and the DPDP's consent mandate.

It would be a great help to courts if judicial authorities had less friction between different courts, simply by defining very clear jurisdictional boundaries and by harmonizing compensation and penalty mechanisms. Interaction mechanisms between the DPB, IT Act adjudicating officers, sectoral regulators, and cybersecurity agencies like CERT-In should be established through consultation and rule-making. Such frameworks would allow for joint investigations, cross-regulatory information sharing, and unified enforcement strategies, thus leading to a higher level of overall regulatory coherence.

Moreover, having India's data protection regulations more in line with global standards would be very helpful in attracting cooperation, trust, and compliance from other countries with whom India does business. The use of universally agreeable methods for handling cross-border data transfers, making adequacy determinations and cooperating for enforcement purposes would eliminate the problem of conflicting jurisdictions and create a uniform global digital ecosystem.

To put it simply, India is a country which is on a decisive point where its data protection regulations need to develop further through gradual tweaking, getting the views of the interested parties and being in agreement with other countries so as to be able to effectively deal with the border conflicts. Such a measure is very important for the protection of privacy rights, a strong data governance system, the attraction of investors and the gaining of the trust of consumers as well as the accomplishment of the full potential of India’s digital transformation. By supporting

 [ISSN 2581-5369]

a well-coordinated, clear and efficient regulatory system, India will be able to become a worldwide leader in handling the complicated interaction between data protection, cybersecurity and sectoral regulations in the digital era.

*****

 [ISSN 2581-5369]

XII. REFERENCES

1. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
2. Information Technology Act, 2000 (Act 21 of 2000).
3. Information Technology (SPDI) Rules, 2011 (under the IT Act, 2000).
4. Srishti Kumar, 'Exploring jurisdictional overlap in India's data protection landscape' (2023) *Bar and Bench*, https://www.barandbench.com/columns/exploring-jurisdictional-overlap-in-indias-data-protection-landscape.
5. Taxmann, 'DPDP Act vs IT Act – Shifting India's Data-protection Paradigm' (2025) *Taxmann*, https://www.taxmann.com/post/blog/dpdp-act-vs-it-act.
6. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) dated April 11, 2011, published in the *Gazette of India, Extraordinary, Part II, Section 3, Sub-section (i)*.
7. Srishti Kumar, 'Exploring jurisdictional overlap in India's data protection landscape' (2023) *Bar and Bench*
8. Digital Personal Data Protection Act, The Schedule, Item 1 (2023).
9. King Stubb & Kasiva, 'Penalties and Adjudication under the DPDP Act, 2023: Powers of the Data Protection Board and Quantum of Fines' (2025) *King Stubb & Kasiva*
10. Press Information Bureau (PIB), Government of India, 'Government notifies DPDP Rules to empower citizens and protect privacy' (2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014.
11. Consent, 'What is the difference between DPDP Act and GDPR?' (2023) *Consent*, https://www.consent.in/blog/dpdp-vs-gdpr.
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1., Cal. Civ. Code § 1798.100 et seq. (West 2018).
13. IAPP, 'Global Privacy Law and DPA Directory' (2025) *International Association of Privacy Professionals*, https://iapp.org/resources/global-privacy-directory/.

14. Ardent Privacy, 'GDPR Vs India's DPDPA: Key Differences And Compliance Implications' (2025) *Ardent Privacy.*

15. Zou Global Services, 'Decoding India's DPDP Act: A Privacy Leader's Perspective' (2025) *Zou Global Services*. See also King Stubb & Kasiva, 'Consent Framework under the Digital Personal Data Protection Act, 2023: Legal Requirements and Compliance Strategies' (2025) *King Stubb & Kasiva.* See also*, Latham & Watkins LLP, 'India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison' (2024) Latham & Watkins LLP.*

16. ANI News, 'Government notifies DPDP rules to empower citizens, protect privacy' (2025) *ANI News*, https://www.aninews.in/news/business/government-notifies-dpdp-rules-to-empower-citizens-protect-privacy20251114215316.

17. Crossing Borders: Comparative Perspectives on Data Protection Laws in India, the EU, and the US' (2024) *Journal of Data and Information Privacy Research* Vol. 1, No. 2.

18. Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (Revised 2015).

19. Organisation for Economic Co-operation and Development, *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(2013)79 (2013).

20. Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems (Schrems II), C-311/18, [2020] ECR I-541, [2020] 2 CMLR 10 (CJEU).

21. Khaira, Rachna, 'Rs 500, 10 minutes, and you have access to billion Aadhaar details' (2018) *The Tribune*; World Economic Forum, 'The Global Risks Report 2019: 14th Edition' (2019) *WEF Global Risks Report*, 37.

22. World Economic Forum, 'The Global Risks Report 2019: 14th Edition' (2019) *WEF Global Risks Report*, 37. *(This report highlights that the breach was due to "lax cyber security protocols," supporting the claim that the cause was governance and access control failure rather than a traditional cyberattack.)*

23. 'The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment' (2019) *Jackson School of International Studies, University of Washington*. https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/

24. Qantas Group, *UPDATE ON QANTAS CYBER INCIDENT: WEDNESDAY 9 JULY 2025* (July 9, 2025) Qantas Newsroom, [URL]; Cyber Management Alliance, *Qantas*

Data Breach: Scattered Spider Takes to the Skies? (July 3, 2025) Cyber Management Alliance Blog.

25. Cyber Management Alliance, *Qantas Data Breach: Scattered Spider Takes to the Skies?* (July 3, 2025) Cyber Management Alliance Blog.
26. Privacy Act 1988 (Cth).
27. Qantas Group, *UPDATE ON QANTAS CYBER INCIDENT: WEDNESDAY 9 JULY 2025* (July 9, 2025) Qantas Newsroom, [URL]; 'CROSS-BORDER DATA PRIVACY AND LEGAL SUPPORT: A SYSTEMATIC REVIEW OF INTERNATIONAL COMPLIANCE STANDARDS AND CYBER LAW PRACTICES' (2025) *American Journal of Scholarly Research and Innovation* Vol. 3, Issue 1, 31.
28. Cyber injunctions put victims at risk, experts warn (October 27, 2025) *Information Age - ACS*. [https://ia.acs.org.au/article/2025/cyber-injunctions-put-victims-at-risk--experts-warn.html]
29. FIR No. 250 of 2022 (Delhi Police, Intelligence Fusion and Strategic Operations Unit) (Invoking sections of the Information Technology Act, 2000, including S. 66F for Cyber Terrorism, and sections of the Indian Penal Code, 1860, including for Extortion).
30. Srivastava, Ashish, 'AIIMS Delhi: Held to ransom by cyberattack' (2022) *The New Indian Express*, 28 Nov. 2022; 'AIIMS Ransomware Attack - Cyber Management Alliance' (July 5, 2023) *Cyber Management Alliance Blog*.
31. FIR No. 250 of 2022 (Delhi Police, IFSO Unit) (Invoking IT Act, S. 66F, and IPC); 'TOPIC: CYBERATTACK ON CRITICAL INFORMATION (CI) INFRASTRUCTURE- A CASE STUDY OF RANSOMWARE ON AIIMS' (2023) *Lukmaan IAS Blog*.
32. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.).
33. FIR No. 250 of 2022 (Delhi Police, IFSO Unit) (Invoking IT Act, S. 66F, and IPC); 'AIIMS Cyberattack - The Aftermath' (2025) *Legal Era Magazine*.
34. 'Global Data Privacy Compliance: Challenges and Strategies for Interoperability' (2024) *Journal of Law, Technology and Policy* Vol. 10, No. 4.
35. 'Regulatory Fragmentation and the Erosion of Individual Data Subject Rights in Cross-Border Data Flows' (2023) *Int'l Rev. L. & Data* Vol. 5, No. 1.

 [ISSN 2581-5369]

36. Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025 (notified Nov 2025) (on operationalization and phased enforcement timelines of the DPB).

37. Srishti Kumar, "Navigating Jurisdictional Intersection in India's Data Protection Regime," Dalaw.in (Mar. 23, 2021); Srishti Kumar, "Exploring Jurisdictional Overlap in India's Data Protection Framework," BarandBench.com (Sept. 27, 2023); ExpressComputer.in, "Enforcement Gaps in India's DPDP Act," (July 2025); AZB Partners, "The Digital Personal Data Protection Act Analysis," (Sept. 2023).

*****

 [ISSN 2581-5369]