THE LEGALITES LEXSCRIPTA
ISSN 3108-2416 (ONLINE)
Editor-in-Chief: - Prof. (Dr.) Aryendu Dwivedi
Volume II Issue II (April-June) Page No.: - 108-119

# INDIA'S DPDP ACT VS THE EU'S GDPR: A COMPARATIVE STUDY

**Author: Chirag Garg, LL.B. (Hons.), 3rd Year Student, Amity University, Noida**

**Co-author: Dr. Tanvi Sharma, Assistant Professor, Amity University, Noida**

## ABSTRACT

In August 2023, India passed its first substantive data protection law, almost five years after the Supreme Court declared privacy as a fundamental right in Justice K. S. Puttaswamy (Retd.) v. Union of India. The Digital Personal Data Protection Act, 2023 (DPDP Act) came into being after a lengthy contentious legislative process that has resulted in the coming up with Justice Srikrishna Committee report, a Bill on Personal Data Protection, a committee in revision and finally this Act. By May 2018, when the European Union introduced the General Data Protection Regulation (GDPR), data protection legislation that had become known as the most popular in the world, it had already been adopted by many individuals.

This dissertation draws parallels of the two frameworks in five dimensions: legislative structure and scope; rights of individuals; duty of those processing data; cross-border transfer measures; and enforcement. The comparison is dogmatic in the approach. The main sources are DPDP Act 2023, the GDPR and the Indian and EU case law on the subject. Secondary sources comprise regulatory advice, parliamentary committee papers and scholarly publications.

The main thesis is that although the DPDP Act is in some way, especially in word choice, structured around GDPR, it is non-cosmetic in several ways. This combined with the lack of a sensitive data category, the more limited rights of data principals as compared to GDPR data subjects, the framework of the Data Protection Board of India as a structural body as compared to the independence requirements imposed on EU supervisory authority, and negative-list model of cross-border transfers all have the effect of coming up with a

framework which is recognisable as GDPR adjacent but not GDPR equivalent.

This absence is particularly relevant in terms of its practical implications as it is the difference between India getting the adequacy decision under Article 45 of the GDPR, which would permit EU personal data to flow to India without any additional protection. The

current form of the DPDP Act 2023 will not measure up to the requirements listed in Article 45(2). The dissertation finishes with certain legislation recommendations and maps those areas that will receive special empirical investigation after the notification of the DPDP Rules.

Another way in which the DPDP Act is placed in the context of the global data protection law trend is in the dissertation. Since the GDPR took effect in May 2018 over sixty jurisdictions have passed or significantly amended their own data protection regulations, and most of them follow the same GDPR-proximate pattern that is reflected in the Act in India. Lei Geral de Protecao Data in Brazil, the Personal Data Protection Act in Thailand, the Personal Data Protection Law in Indonesia, and the Decree on Personal Data Protection in Vietnam all heavily rely on the concept of GDPR although they adjust the institutional framework to the specific political and constitutional environment in the country. The experience of India is thus not just a bilateral issue on the EU-India data flows. It is also a case study of the boundaries and constraints of the GDPR diffusion as a model of global data regulation, and the recurrent conflict between embracing a rights-protective lexicon and establishing the institutional framework that the lexicon would allow to be enforced.

The applied interest of this analogy is not just limited to any scholarly fascination with comparative law. The Indian digital economy is one of the largest in the world and the amount of personal information that goes on flow between India and European Union by technology services, business process outsourcing and cross border employment arrangements is huge. The legality of such flows has an impact on millions of citizens whose information is at stake, thousands of companies that do business in both jurisdictions, and governments that must deal with a more convoluted spectrum of data governance. The nature of those flows in years to come, should India be allowed to receive an adequacy decision under Article 45 of the GDPR, will have a direct impact on the structure of such flows, and will directly influence the costs of compliance, contractual architecture and bargaining power by both parties in the context of the wider EU-India Trade and Technology Council.

This comparison highlights a trend that is now widely used in the literature on comparative data protection: a jurisdiction that borrows the GDPRs lingo and overall framework without reproducing the institutional and rights framework that provides that lingo with the semantics of life. Terms familiar to any GDPR professional, such as data fiduciary, data principal, consent and processing can be used in the DPDP Act but in a framework that does not

necessarily immediately present itself via a surface reading when compared to the GDPR. The current dissertation provides those differences on a tangible scale, evaluates their legal implications, and checks whether the overall extent of protection provided by India is, in the terminology of Article 45(1) basically the same as that provided under the European Union.

***Keywords:*** *DPDP Act 2023, GDPR, data protection, adequacy decision, Data Protection Board of India, comparative law, India privacy law, cross-border data transfers.*

# CHAPTER 1 - INTRODUCTION AND STATEMENT OF PROBLEM

## 1.1 Background and Context

In August 2023, India enacted a Digital Personal Data Protection Act. That is a misleadingly innocent sentence. The Act had been long overdue, stalled out through a series of conflicting issues which were both substantive on the one hand, and both political and, in some cases, mere bureaucratic. By the moment it actually came to pass, much had evolved in the technology scene, global information control and the constitutional knowledge of the Indian constitution about privacy.

The book begins, in a significant meaning, with a Supreme Court bench comprising of nine judges. In Justice K.S. Puttaswamy (Retd.) v. Union of India[1], the court in August, 2017 unanimously stated that the Indian constitution guaranteed the right to privacy through Articles 14,19 and 21, as a fundamental right. Some observers were predicting that ruling, but its extent astonished many. The court was not simply issuing informational privacy at a bow; various concurring views discussed it, and that of Justice D.Y. Chandrachud specifically gave a framework upon which it would be referred to in the proceedings relating to data protection bill.

The bottom floor of the constitution was Puttaswamy. Non-legislative constitutional rights do not have the flexibility to do much with non-state actors, businesses, services, and data brokers who are not organ organs of the state. In 2017 the government had already formed the Justice B.N. Srikrishna Committee to draft a data protection bill; since the result of Puttaswamy, the undertaking of that committee was more urgent. In 2018, the committee released its report that suggested a complex system of personal data protection based expressly on the GDPR that had been adopted in May of the same year.[2]

What that entailed was, as it were, a lengthy procedure. A Personal Data Protection Bill 2019 was presented in Parliament and sent to a Joint Parliamentary Committee. In December 2021, the JPC announced its plan to make major amendments after hearing a number of witnesses who presented compelling evidence and testimony.[3] In August 2022, the government withdrew the bill in its entirety due to the broad changes required, and released a new draft

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[2] Ministry of Electronics and Information Technology (MeitY), Government of India, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018). Available at: https://meity.gov.in/
[3] Joint Committee of Parliament on the Personal Data Protection Bill, 2019, Report (December 2021).

Digital Personal Data Protection Bill in November 2022. It was then followed by a period of public consultation and the DPDP Bill 2023 was introduced and passed in both houses of Parliament in August 2023.

The course of the European Union was other and quicker. Intended to streamline data protection regulations across EU member states, the GDPR substituted the Data Protection Directive 95/46/EC and broadened the rights of individuals and provided an accountability framework that the Directive had never truly reached. Reg. 2016/679 has come into force in May 2018. Since that time, it has assumed, perhaps, the foremost power as a data protection tool in the world not to the degree that it is imitated by others but as a standard by which others are judged.[4]

The digital economy has increased significantly during the time between the Directive and the GDPR, and between the GDPR and the DPDP Act. The magnitude of personal data processing today, in cloud computing, social media, finance-technology, health-app technology and algorithms, is fundamentally unlike what was the case at the time that the Indian IT Act 2000 was written. The clauses of that statute involving the protection of data, contained in the Section 43A and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, never served the purpose. To a more or less extent, everyone was in consensus with this. The issue of disagreement was on what to replace them.

This dissertation makes no attempt to give full legislative history of the DPDP Act. History of that has been ably done elsewhere, and the main concern here is given primarily the text of the law as promulgated, its relation with the GDPR to particular questions, in what respects they are different, and what such differences entail in practice and in law. The comparison practice is not just academic. It is significant to EU-India data flows, the future possibilities of an adequacy decision, and to the compliance requirements of multinational organizations based in both jurisdictions.

It is worth mentioning the geopolitical context of the adequacy question as well. Adequacy assessments conducted by the European Commission are not essentially technocracy exercises. They are played in a context of trade relations, diplomatic factors, and strategic interests. The announcement by the EU in 2021 to award the United Kingdom adequacy,

[4] Graham Greenleaf, Global Data Privacy Laws 2023: 162 National Laws & Bills (2023) 181 Privacy Laws & Business International Report 5-8.

despite substantial worries during the UK about its surveillance laws, was challenged by privacy experts just because it seemed to be politically convenient rather than legally sound. The increased role of India as a technology partner and the momentum of the EU-India Trade and Technology Council negotiations leading to a political discussion where an adequacy decision can be desirable independent of the strict legal requirements being fulfilled. The dissertation will disregard such political considerations, and concentrate on the legal examination, though their presence must be considered in judging the likelihood of eventual adequacy being forthcoming.

This is not the only position of India. The Personal Information Protection Act of South Korea was initially adopted in 2011 and underwent major adjustments in 2023, prior to receiving an EU adequacy determination. The Act on the Protection of Personal Information in Japan was extensively reformed between its original adoption in 2003 and the 2019 adequacy decision by the Commission, and even then, the decision was subject to additional rules adopted by the Personal Information Protection Commission of Japan which exceeded the requirements of the local law. The moral of both these comparators is that the adequacy is not attained through the passing of a GDPR-like law: the adequate institution-building, the enforcement culture, and the interpretive practice that is the meaning of the statute in practice. The DPDP Act of India is only the beginning of that process and not the end.

It is helpful to think for a moment on context for GDPR creation, as this shows the difficulty which any place trying to make their law similar to GDPR will face. GDPR was not drafted in isolation. It came after almost four years EU lawmaking negotiations, which was after having about twenty years from the 1995 Data Protection Directive, and also formed by large case law by Court of Justice. Article 29 Working Party, who later changed to European Data Protection Board, already gave out many opinions and guidelines, so definition for the Directive in practical sense got set. When GDPR began to be used, there was shared culture between the European data protection authorities, already established case law, and community of practitioners having strong connection with base laws. No country making first time data protection law can copy that much background context, DPDP Act is not outside from this reality.

### 1.2 Statement of Problem and Research Gap

By now, literature about GDPR is, to put blunt, huge. There are commentaries, casebooks, regulatory guidance, also judicial judgments, that together make big amount of analysis. But

writing on DPDP Act 2023 is much smaller, which is expected, since Act is new, rules are still not notified, and India Data Protection Board still not started work.

From this, more difficulties come. First, most comparative writing is from before DPDP Act was passed, so those comparisons were basically only hypothetical. Second, early studies after law came sometimes only see the places that are same to GDPR, which is true, but do not always explain the structural parts that are different. Third, and most importantly, not any study has actually used Article 45(2) GDPR rules to check if DPDP Act 2023 is enough for adequacy. This gap is very significant because the topic about adequacy will likely be important in EU-India digital market discussions soon.

So clearly, this dissertation's research gap is very clear: comparing doctrinally the DPDP Act 2023 and GDPR after DPDP passed, and looking strongly to differences in structure and how those affect examination for Article 45 adequacy. The comparison is made for five subjects: scope and definitions; legal basis for processing; individuals' rights; how institutions are made; and enforcement and transfers, selected because these line up with what European Commission has used of criteria for adequacy before.

The way of doctrine study in this work is to compare clearly particular law parts, not only wide description of themes. For each of the five subjects, method is threefold: first find the GDPR rules and explanations for them; then find DPDP Act versions; after that check if they are functionally same or actually different. If any differences are there, the study asks, is it because of they wanted it that way with policy, is it a missing thing, or is it postponed on purpose for more rules later. These separations are important because they decide how or also if both systems can get closer in future.

Using adequacy decision criteria as main analytical method needs justification, since one can argue adequacy alone is too limited for review of domestic data protection legal act. DPDP Act is still mostly Indian law for Indian people, not a rule made for making European regulators happy. In this sense, much more significant are questions like if Act gives enough protection to Indian data principals' interests, if enforcement is practical by Indian regulatory system, also the compatibility with framework of India's Constitution. These are all valid points, and it must be said that they are not dismissed in this thesis. Still, the adequacy angle has some special analytical purpose: Commission over many adequacy decisions and by EDPB's advice reports has developed in public a quite detailed list of criteria for measuring Act's provisions. This makes analysis specific and not simply impression-like, grounding the

checking in legal standards and not only abstract judgements on whether Act can be seen as 'good enough'.

### 1.3 Research Questions

There are three main research questions working as the organisation of this dissertation:

First: How far DPDP Act 2023 is fitting with the substantial and institutional requirements for GDPR? This is being descriptive nature question. It will need careful reading with both acts side-by-side and truly report about where they say the same things, where it speaks differently, also places where DPDP Act has only silence when GDPR is addressing the subject.

Second: In cases where two frameworks are in divergence, what could be law consequences as well as commercial on data principals, data fiduciaries and operator doing business in more than one country? This is coming as analytical type question. All divergences are not same level of importance. Some are result of intent policy decisions, like India is choosing a different way towards legitimate interests, while some are just due to drafting empty parts or postponed on onwards secondary regulations.

Third: Is DPDP Act 2023 achieving the required threshold as per adequacy decisions coming under Article 45 in GDPR? This can be seen as evaluative question. It is needed that criteria in Article 45(2) should be applied and that those earlier adequacy decisions must be studied for how Commission has put them into practice through the application of those criteria.

### 1.4 Research Objectives

The goals which relate to these questions are to make maps and to compare structure architecture for both frameworks, based on five identified dimensions; also, to find places of convergence, where there are gaps, and substantive conflicts existing in between them; and to check India's adequacy and preparation then create legislative suggestions that could resolve problems which are identified.

Another target, existing in the dissertation but not in one part only, is putting the comparison in more a global privacy convergence context, so in the recent trend of data protections laws created from 2018 onwards that use GDPR-related language but do not take in full GDPR structural elements. India does not stand alone inside this. Some other countries like Brazil's LGPD, PDPA from Thailand, South Korea with PIPA (amended), and more are showing alike

patterns. The relationship of DPDP Act for GDPR is partly a specific bilateral matter and is also an example of a broader happening. Mapping the Indian situation with these similar ones is one of additional aims for analysis to follow, for to understanding DPDP Act while seeing into the world-wide context gives visibility for both what are the choices made already, and what are possible for Indian lawmakers when thinking about next amendments that are needed for adequacy at the end.

### 1.5 Hypothesis

Two hypotheses get tested:

H1: Although DPDP Act 2023 is using concepts and terms derived from GDPR, some structural gaps, mainly for the independent supervisory authority, covered scope for individual right, none sensitive data category, also the construction of transfer systems, are probably to make India not able to get GDPR adequacy decision (Article 45) soon.

H2: These lacking in structure are leading to one-sided compliance duties to multinational corporations, who must do two separates not working together compliance plans, one for GDPR and one for DPDP Act.

H1 is maybe called a limited convergence proposal: converging at language and divergent for structure. H2 is more on practical effect. Both will be tested in Chapter 3 through to Chapter 5, with conclusion given in Chapter 6.

It is important to say both hypotheses are not logically depending on each other. H1 is about the tie between DPDP Act and GDPR when looking for structure and rights. H2 relates with what effects in practice this has for the multinational companies to comply. It is possible theoretically to get confirmation for H1, like structure divergence means adequacy is not possible, but at the same time see H2 not confirmed, maybe because all divergences go in similar direction so GDPR compliance is also enough for DPDP Act in most cases. However, as seen from what Chapter 4 is showing, this is not a real pattern: the differences really are not equal, making new requirements which move in different directions and cannot be matched by just one compliance plan made for either only.

A remark should be said what these hypotheses do not state. Not H1 or H2 claims DPDP Act is designed poorly or that it does not protect Indian data principal. Adequacy is a particular and quite demanding standard: it asks if India’s framework gives protection basically equal with GDPR, which is checked based with criteria mainly looking at EU data subjects’ rights

when their data move into India. Framework, it can be really protective of its own citizens but still not be adequate according to Article 45(2) just for letting free movement of EU-India personal data. It is a key difference, and this distinction is kept in all the analysis that comes next.

### 1.6 Research Methodology

This dissertation uses doctrinal legal research for main methodology. The comparative approach is analytical and critic, not empirical; so, no survey is made, no interviews or field study. Main legal sources consist of Digital Personal Data Protection Act, 2023, General Data Protection Regulation 2016/679, Information Technology Act 2000, IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Justice B. N. Srikrishna Committee Report from 2018, Joint Parliamentary Committee Report on Personal Data Protection Bill (2021), guidelines and opinions from European Data Protection Board, Supreme Court of India cases and case law of European Union Court of Justice.

Secondary sources involve peer-reviewed journals, several books, MeitY consultative documents, papers by NITI Aayog, annual reports and opinions from national data protection authorities in areas having GDPR adequacy status. When secondary legal sources are cited, top preference given to the ones which cite their own primary sources specifically.

Comparative method is borrowed from how it works of public law comparatism: to identify function a rule is having, describe what institutional context it works, after which you compare rule with the parallel one in the other system at the function level, not only side-by-side wording.[5] Looking similar wording can mask different function; DPDP Act and GDPR show that for example.

Few limitations must be pointed at early. DPDP Rules have not been notified until the writing of this text. Act gives huge powers for rulemaking to central government, so list like details of how the framework works, where data cannot be sent, duties of Significant Data Fiduciaries, constitution or process of Data Protection Board will be with by-laws which text is still not known. This analysis is for that reason only temporary for some ways. Second, this dissertation does not add empirical study: it does not try to find about compliance costs, review regulatory ability, or do surveys for what practitioners think. These issues are important, are marked for future research in Chapter 6.

[5] Konrad Zweigert and Hein Kotz, An Introduction to Comparative Law (3rd ed., Oxford University Press, 1998) pp. 34-47.

### 1.7 Structure of the Dissertation

Chapter 2 discuss the literature, scholarship about GDPR, talk about Indian privacy law area, comparative data protection and points out the exact gap that this research wants to cover.

Chapter 3 compares in detail the architectural features of the two legal frameworks: their respective scopes, the legal definition of what constitutes ‘personal data’, the legal bases upon which processing is permitted, and the institutional design of each framework.

Chapter 4 will examine in detail individual rights (the rights of data principals/data subjects) with the associated obligations of those who process personal data.

Chapter 5 examines the methods by which personal data can be transferred across international borders; examines the enforcement provisions of the two frameworks; and considers whether or to what extent an appropriate level of protection exists for transfers from one jurisdiction to another under Article 45 of the GDPR.

Chapter 6 summarizes the findings of this study, evaluates the validity of the hypotheses advanced at the outset, outlines detailed legislative proposals, highlights limitations, and provides a map for potential future research.