BRAWIJAYA LAW JOURNAL
Journal of Legal Studies
e ISSN 2503-0841
p ISSN 2356-4512
Volume 9 No 1, April 2022
Nationally Accredited No. 164/E/KPT/2021 Dated 27th December 2021

The Passport to Regulate Foreign Jurisdiction: The Personal Data Protection Bill, 2019 on its Extraterritorial Application

Vasishtan P.

Hidayatullah National Law University, Raipur, India
Email: vasishtan98@gmail.com

DOI: http://doi.org/10.21776/ub.blj.2022.009.01.04

Submitted: 2021-09-10 | Reviewed: 2022-03-24 | Accepted: 2022-04-13 | Published: 2022-04-30

How to Cite: P, Vasishtan. 2022. "The Passport to Regulate Foreign Jurisdiction: The Personal Data Protection Bill, 2019 on Its Extraterritorial Application". *Brawijaya Law Journal* 9(1):47-58. https://doi.org/10.21776/ub.blj.2022.009.01.04.

Abstract: *The Indian Personal Data Protection Bill, 2019 (PDP Bill) was formulated from the Recommendations of the Justice Srikrishna Report. This Bill was the first portkey for India's exclusive data protection regime. Notably, there is an urgent need to establish a strong legal framework for data protection in India as this would be the only safehouse for protecting every individual's personal data, including sensitive and critical data. The EU's General Data Protection Regulation (GDPR) serves as a yardstick for global data protection regulation due to its architecture that places a great onus of compliance on foreign entities. This resolute extraterritorial nature that GDPR thatches on itself has inspired several upcoming worldwide data protection regimes. Consequently, the Joint Parliamentary Committee, which is tasked with reviewing India's PDP Bill, has the responsibility to upgrade its stance to be tenacious and more obstinate, as well as ensure that the Bill has a strong extraterritorial foundation. This requirement comes with a plethora of challenges under international law as questions on cross-border jurisdictions are inevitable. This paper compares the PDP Bill with the GDPR and Brasil's Lei Geral de Proteção de Dados (LGPD) and analyzes the key challenges emerging from the extraterritorial scope of these legislations through the lens of international law. Its main objective is to identify the possible and plausible solutions to these extraterritorial jurisdictional issues and highlight how the fundamental construction of India's PDP Bill can be improved to effectively address the extraterritorial concerns.*

Keywords: *Data Protection, PDP Bill, Extraterritorial Application, GDPR, LGPD, International Cooperation.*

I. Introduction

A state assumes the responsibility of its citizens and residents' safety within its jurisdiction.[1] However, when there is need to safeguard the interests of its citizens who

[1] The concept of 'jurisdiction' in the field of protection of citizens has also developed its own independent meaning, not considered in this article, which recognises that states may have extraterritorial human rights obligations based on effective control over territory or persons. A state in unlawful occupation of territory may thus be subject to jurisdictional *obligations* under human rights law, even though it lacks jurisdictional *rights* as a matter of general international law. See generally e.g., Marko

reside in other jurisdictions, international law comes to play.[2]

International law serves as the yardstick for regulating international relations, thereby promoting global peace and prosperity and ensuring that states are able to protect the best interests of their citizens elsewhere while maintaining their sovereignty and integrity.[3] This is a subject matter jurisdiction.

Jurisdiction is the legal authority a state or an international body possesses over a territory of land, air, water etc., to exercise its authority over that region. Jurisdiction is a part of globe that is devoted and subjected to a state's sovereignty.[4] Only a few widely ratified conventions, such as the Vienna Convention,[5] provide for limited diplomatic exemptions to these scenarios.

As Oppenheim opines, "States possessing independence and territorial as well as personal supremacy can naturally extend or restrict their jurisdiction as far as they like."[6] This opinion remains valid as long as records to any trade deals across borders are well documented in pen and paper. However, with the advent of the digital era, the pen and paper trade deals have been replaced with other digital methods. The pervasive cyberspace concept has decentralized the notion of borders and territories and prompted a paradigm shift regarding jurisdictions over cyberspace matters.[7]

The decentralization of the demarcated sovereign borders by the internet has subsequently opened doors for worldwide regulators and courts to apply the "extraterritorial effect." Notably, the extraterritorial effect of national legislation and policies was an issue of concern even before the era of the internet.[8] Privacy laws, especially those protecting the personal data of citizens and individuals, are the newest addition to the extraterritorial regulations that states promulgate to protect the interests of their subjects and exercise their sovereignty.[9] This scenario raises two prima facie questions on the regulators and the courts: How aware are the states to avoid detrimental and redundant impact across their borders and can would they minimize such adverse effects?[10]

Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (OUP, 2011).

2 *SS 'Lotus' (France v Turkey)* (1927) PCIJ Ser A, No 10.

3 *UK vs. Norway* (North Atlantic Fisheries Case), [1951] ICJ Rep.116.

4 James Crawford, *Brownlie's Principles of Public International Law*, 8th edn (OUP, 2012); D. W. Bowett, "Jurisdiction: Changing Patterns of Authority Over Activities and Resources," *BYIL* 53, no.1 (1982). 53 BYIL 1, 1, describing jurisdiction as 'a manifestation of State sovereignty'

5 Vienna Convention on Diplomatic Relations 1961, Done at Vienna on 18 April 1961. Entered into force on 24 April 1964. United Nations, Treaty Series, vol. 500, p. 95.

6 Oppenheim, International Law, Chapter 1, s.143. Even Oppenheim, however, followed this by stating that 'as members of the Family of Nations and International Persons, the States must exercise self-restraint in the exercise of this natural power in the interest of one another', and (implicitly recognising the disparity between the 'positivist' perspective and accepted practice) went on to treat jurisdiction as based strictly on territoriality and nationality (with the exception of piracy), arguing that even passive personality was an impermissible extension of jurisdiction.

7 Jean-Baptiste Maillart, "The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime," *ERA Forum* 19 (2019). https://doi.org/10.1007/s12027-018-0527-2.

8 The United States of America's Helms Burton Act, regulated on the bribery or unauthorised sanctions relating to third countries, had an extraterritorial effect defacto by nature.

9 "The Internet and Extra-Territorial Effects of Laws Internet Society Concept Note," Internetsociety.org, accessed April 11, 2021, https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws-EN.pdf.

10 Id. at page 3.

This paper analyzes the extraterritorial aspect of India's Personal Data Protection Bill, 2019 ("PDPB")[11] and attempts to compare it with the European Union's General Data Protection Regulation ("EUGDPR") [12] and Brasil's Lei Geral de Proteção de Dados ("LGPD")[13]. As the PDPB is under scrutiny before the Joint Parliamentary Committee[14] prior to its promulgation into an Act, this article may help shade more light on any gray areas in the Bill. The overarching idea is to examine how the PDPB's extraterritorial position will ensure personal data protection.

II. Legal Materials and Methods

The main materials used in the current study are the EU's GDPR, Brasil's LGPD, and India's PDP Bill, 2019. The research carried in this study is non-empirical and doctrinal in nature. The main sources of information were Acts, books, commentaries, and online news and journal articles that support the research idea and questions pursued in this study. The research mainly focused on India's position on the extraterritorial application of its data protection regime as compared to the preceding EUGDPR.

III. Results and Discussion

The Personal Data Protection Bill, 2019

a. Understanding the Bill

The PDPB was formulated from the recommendations of the Justice Srikrishna Committee's Report on Data Protection[15] is intended to govern entities that process personal data. These entities include the Government, companies that are incorporated in India, and foreign companies that deal with Indian citizens'' personal data. The type of data covered under the Bill includes personal data that contains the characteristics, traits, and attributes of identity that can identify an individual. [16] There are certain subsets of data that are categorized as sensitive personal data ("SPD") in the PDPB, which include data pertaining to financial information, biometrics, caste, and religious and political affiliations of an individual.[17] There is also

[11] The Personal Data Protection Bill, 2019 was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on 11 December 2019. The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same. 4173LS(Pre).p65, accessed April 11, 2021.

[12] The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas. "General Data Protection Regulation," accessed April 11, 2021, https://gdpr-info.eu/.

[13] The General Personal Data Protection Law 13709/2018, is a statutory law on data protection and privacy in the Federative Republic of Brazil. The law's primary aim is to unify 40 different Brazilian laws that regulate the processing of personal data.) LGPD-english-version.pdf (lgpdbrasil.com.br), accessed April 11, 2021.

[14] The PDP Bill, 2019 was referred to the Joint Parliamentary Committee by the Indian Parliament in its initial attempt to pass it in the House. The JPC is headed by Ms. Meenakshi Lekhi. Committee: Loksabha (loksabhaph.nic.in), accessed April 11, 2021.

[15] The Srikrishna Report was drafted with a belief that the protection of personal data holds the key to empowerment, progress, and innovation of not only India, but also the Indians. The report intended to adopt learnings from best practices that exist in developed democracies with considerably advanced thinking on the subject. Committee Report on Draft Personal Data Protection Bill, 2018_0.pdf (prsindia.org), accessed April 11, 2021.

[16] "The Personal Data Protection Bill, 2019" prsindia, accessed April 11, 2021, https://prsindia.org.

[17] §2(36), The Personal Data Protection Bill, 2019 was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on 11 December 2019. The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same. 4173LS(Pre).p65; other factors include sex life; sexual orientation; genetic

another subset called as critical personal data ("CPD"). The PDPB stipulates that the Government will define this type of data through notices.[18]

b. The Extraterritoriality Provisos Available in the PDP Bill, 2019

§2(c) of the PDPB states that the applicability of the Act with respect to the processing of data shall apply to

"*… (c) the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is —*

(i) … any systematic activity … to data principals within the territory of India; or
(ii) … which involves profiling of data principals within the territory of India…"

This provision expressly confirms the extraterritorial applicability of the PDPB. Therefore, India's discretion to hold any data fiduciary liable in the event of these conditions is wide. This is a welcome expansion as the previous IT Act and the SPDI Rules left a gray area in terms of their extraterritorial applicability.[19]

§33 allows SPD to be transferred outside India but prohibits those transferring it from storing it and strictly advices that CPD only be processed in India, unless the Government authorizes otherwise or there is a health emergency. It is also important to note that the word "transferred" does not mean "processing" under §3(31)[20].

§34 provides for conditions under which the transfer under §33 can be effected; i.e., when explicit consent of the data principle[21] is present and the transfer is approved by the authority,[22] which has the responsibility to ensure that the rights of the data principal are protected, the data fiduciary[23] is liable for any non-compliance, and the protection of the data itself complies with all laws and agreements. Under §50, the authority strictly considers compliance to §34 as a good practice under its code of practice[24].

On the penal aspect, §57 penalizes the data fiduciary if it contravenes any provisions of the Act with a minimum fine of ₹15 Crores or 4% of the total worldwide turnover of the Fiduciary for the previous year.[25] This provision confirms that a data fiduciary can be a foreign company and, therefore, the PDPD has extraterritoriality over foreign companies handling Indians' data. Notably,

data; transgender status; intersex status; caste or tribe; or any other data categorised as sensitive personal data under §15

18 §33, The Personal Data Protection Bill, 2019 was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on 11 December 2019. The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same. 4173LS(Pre). p65.

19 Harish Walia and Supratim Chakraborty, "Indian Data Protection Law," iclg.com, n.d., accessed April 11, 2021, https://iclg.com/practice-areas/data-protection-laws-and-regulations/india.

20 §3(31) — "processing" in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

21 §3(14) — "data principal" means the natural person to whom the personal data relates.

22 §3(5) — Authority" means the Data Protection Authority of India established under sub-section (1) of §41.

23 §3(13) — "data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;

24 §50(6)(q) — Codes of Practice – The code of practice under this Act may include the following matters, namely, transfer of personal data outside India pursuant to §34;

25 §57(2) read with §57(3)(a). — Penalties for contravening certain provisions of the Act.

the same has not been mentioned under §3(13), which defines a data fiduciary.

It is also important to note that the Act can only be invoked on such processing of data within the territory of India. There is no express protection on Indian citizens or residents per se. Even if data processing occurs in India, or is carried by foreign data fiduciaries on data supposedly processed in India, the Act does not invoke any beyond this aspect.

Comparative Law on Extraterritoriality: The GDPR & LGPD

The concept of extraterritoriality is a foremost safeguard that can be applied to data processing and handling.[26] Since the internet realm has decentralized borders, the only solution and wall of defense to protect an individual's data is to allow the law to follow the data regardless of where the data fiduciary/processor is located.[27] This way, an individual can carry one part of the sovereignty of their state and their best interests can be protected. This can be effected by the extraterritorial applicability of data privacy laws.

a. Convergence of laws in Foreign Jurisdictions

GDPR and LGPD enable a free-flow of data courtesy of the laws formulated as such. This means that both LGPD and GDPR impact personal data and allow processing without a local, physical presence of the data subjects.[28] Consequently, this helps data fiduciaries to understand the big data of the EU better. This would create a positive impact on businesses that target big data and their relevant consumers.[29] This is one aspect where India may be lacking. Data that exists and is stored within India may be safeguarded, but it is a one-way corridor when the data belongs to an Indian residing abroad and the data fiduciary also exists outside the territory of India. When a foreign data processor processes data of an Indian citizen who lives outside India, which was not processed inside India, the Central Government has powers to exempt the application of the PDPB.[30] This may cause a great deal of loss to Indian fiduciaries processing data from outside India, which would subsequently impact the global race that countries participate in as they endeavor to process the global big data.

b. Nodal Authority

The concept of SPD has always been of paramount importance even before the digital era in the European Union Nations, better than India[31] or Brasil[32]. In terms of the

[26] "The Internet and Extra-Territorial Effects of Laws Internet Society Concept Note," at 12.

[27] Bruno. R. Bioni, "A Produção Normativa a Respeito Da Privacidade Na Economia Da Informação e Do Livre Fluxo Informacional Transfronteiriço," in *Direitos e Novas Tecnologias: XXIII National Meeting of Conpedi, 1*, 2014, 59–82, accessed April 12, 2021, https://brunobioni.com.br/wp-content/uploads/2020/02/internet-sectoral-overview-xi-2-privacy-7-11.pdf.

[28] "Brazil's New Data Protection Law: LGPD Marketer's Guide," SaaSholic, accessed April 12, 2021, https://www.saasholic.com/

[29] Id.

[30] §37 – Power of Central Government to Exempt Certain Data Processors — The Central Government may, by notification, exempt from the application of this Act, the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.

[31] "The Internet and Extra-Territorial Effects of Laws Internet Society Concept Note," at 43.

[32] Comparing GDPR v. LGPD, OneTrust DataGuidance, B.Luz, Advocates. "gdpr_lgpd_report.pdf", Dataguidance, accessed

appointment of a nodal officer, the PDPB stands far superior than the other two. The LGPD is more restrictive in nature when it comes to public health data or transfer of data to any processor or fiduciary outside the jurisdiction of the law.[33] The appointment of a data protection officer ("DPO") by a data fiduciary[34], irrespective of their location, is a key improvement in the PDPB that is missing in both the GDPR and LGPD. However, the GDPR also provides for provisions [35] to appoint a DPO, but it is restrictive in nature and it can only be applied under certain conditions of controlling data. The significance of a DPO is seen in cases where the data fiduciary is acting outside the scope and powers prescribed to it by the local data provisions. In the PDPB scenario, the appointment of a DPO has positive effects; i.e., it ensures that authorized personnel are held liable before a competent Indian authority in case a foreign fiduciary defaults. The position of the EU and Brasil is better safeguarded as the reach of extraterritoriality as their regulations are longer and more expansive in nature. However, the question of trying a defaulter before an authority in the event of a default is still a gray area.[36]

c. The Significant Reach of Extraterritoriality

Perhaps the most significant contrast where the GDPR and LGPD take a superior lead over the PDPB is how the extension of the extraterritorial arms has been formulated. Article 3 of the GDPR vests the jurisdiction to the data controller and the processors in the EU, regardless of where data processing takes place. [37] This is also present in the LGPD as it was inspired by the ideals enshrined by the GDPR. [38] However, the PDPB misses out on this important aspect. This gives rise to a situation where if data fiduciaries were to process data of a citizen or an individual belonging to the EU Nations, even when such data subjects do not presently reside in the EU region, the fiduciaries would still be required to comply with the GDPR.[39]

On the contrary, if a data fiduciary is headquartered at Geneva, Switzerland, and it processes data of an Indian citizen living in Europe or even in Chennai, such data fiduciary will not be required to comply with the provisions of the PDPBThis aspect is also missing in the LGPD. However, the LGPD provides that if a foreign data fiduciary is processing data of a Brazilian individual residing inside the Brazilian territory and the data is stored outside of Brazil, the data fiduciary will have to comply with the LGPD.[40] The LGPD applies[41] if the purpose

April 12, 2021, https://www.dataguidance.com/sites/default/files/gdpr_lgpd_report.pdf.

33 Id.

34 §30(3) — The data protection officer appointed under sub-section (*1*) shall be based in India and shall represent the data fiduciary under this Act.

35 Section 4 – Data Protection Officer — Article 37 – Designation of a Data Protection Officer.

36 Glory Francke, "Time to Update Your Privacy Statement For GDPR," *Law 360*, n.d., Comparing GDPR v. LGPD, OneTrust DataGuidance, B.Luz, Advocates. "gdpr_lgpd_report.pdf", Dataguidance, accessed April 12, 2021, https://www.dataguidance.com/sites/default/files/gdpr_lgpd_report.pdf.

37 Article 3 – Territorial Scope — This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

38 Christian Perrone, "Privacy and Data Protection - From Europe To Brazil," n.d., https://doi.org/http://dx.doi.org/10.17768/pbl.y6.n9-10., p82-100.

39 "Brazil's New Data Protection Law: LGPD Marketer's Guide," SaaSholic, accessed April 12, 2021, https://www.saasholic.com/.

40 Ibid.

41 Article 4 of the LGPD.

of an entity's processing activity is to offer or provide goods or services to individuals located in Brazil.[42]

d. Monitoring External Data Fiduciaries

The GDPR is applicable to entities that are not a part of the EU as well as data of individuals who are not EU citizens but are living in the EU.[43] Although the LGPD can be applied on external data fiduciaries, the data subjects must be the naturalized citizens of Brasil.[44] It is worth noting that the PDPB does not define who a data principal in relation to Indian citizenship is. §2(14) only describes a data principal as a natural person on whom the data is being processed.[45]

Key Challenges Emerging Out of Extraterritoriality

The rewards of extraterritorial jurisdiction result in certain equally challenging situations where personal data protection regulations get trapped in endless verticals of the international law and customs. From compliance issues to the overlapping of two jurisdictions, a plethora of diplomatic problems arise while enforcing data protection regulations whose scope has a significant extraterritorial reach.

a. Applicability of the Regulation & Limited Support from International Law

Reiterating the Lotus Principle[46], it states "*a wide measure of discretion (…) to adopt the principles which it regards as best and most suitable*," albeit it is problematic to justify jurisdiction when the GDPR, PDPB, or LGPD decentralizes borders and territories. However, the ideals of international customs are to enumerate laws that civilian states preach and practice[47]. This is a source of law as defined by Article 38 of the ICJ[48]. Moreover, the protection of privacy is thematically well-illustrated by the UDHR[49] and ICCPR[50]. Therefore, the solution lies in interpreting Article 38 first, followed by the privacy protection principles of the treaties.

To fulfill international customs, the justification of the territorial principle will suffice because it is universal and only the location of occurrence matters[51]. Since the breach of the data protection requirement for an Indian residing outside India will not invoke the effects doctrine[52], as the nation where the breach occurs remains unharmed, the passive personality principle would aid the Indian victim who is affected outside the

[42] The LGPD also applies, irrespective of the location of an entity's headquarters, or the location of the data being processed, Comparing GDPR v. LGPD, OneTrust DataGuidance, B.Luz, Advocates. "gdpr_lgpd_report.pdf", Dataguidance, accessed April 12, 2021, https://www.dataguidance.com/sites/default/files/gdpr_lgpd_report.pdf.

[43] Recital 2 of the GDPR

[44] Article 4 of the LGPD.

[45] §2(*14*) "data principal" means the natural person to whom the personal data relates;

[46] Supra Note **Error! Bookmark not defined.**.

[47] Dan Jerker B. Svantesson, "The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses," *Stanford Journal of International Law* 50, no. 1 (2014): 53–102. P. 58.

[48] Article 38 of the International Court of Justice — the legitimacy of extraterritorial claim may be assessed in light of "*international conventions […] establishing rules expressly recognized by the contesting states; international custom, as evidence of a general practice accepted as law; (and) the general principles of law recognized by civilized nations […]*",

[49] Universal Declaration of Human Rights

[50] International Covenant on Civil and Political Rights

[51] "*Nottebohm Case (Liechtenstein v. Guatemala); Second Phase*", International Court of Justice (ICJ), 6 April 1955, accessed April 12, 2021, https://www.refworld.org/cases,ICJ,3ae6b7248.html.

[52] Svantesson, "The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses."

territory of India.[53] However, Article 3(2)[54] of the GDPR and other similar provisions of the LGPD enumerate that this is largely based on the effects' doctrine, whose process is more controversial, as it places complacence on the location over the victims. Since GDPR applies unilaterally across the world, and more in the EU region, this expansiveness may help satisfy the international custom requirement.[55]

The subsequent challenge is to ensure that the PDPB adheres to the general principles of law, as recognized by civilized states.[56] Since states are yet to develop an in-depth understanding of data protection laws ("DPL"), taking precedents from other DPL jurisdictions may help establish the validity of the PDPB, GDPR, and LGPD. For instance, the 2012 Singapore PDP Act applies to entities unilaterally, regardless of whether they were established in Singapore or not.[57] Further, the 1988 Australian Privacy Act[58] applies to any entity that is based out of Australia, and the United States' Foreign Corrupt Practices Act [59] extends to jurisdictions where it may not have territoriality to safeguard the best interests of the intention of the law. All these laws illustrate how DPL can apply anywhere under the general principles of international law.[60] Every nation would want to expand its DPL's extraterritorial scope to affirm its international sovereignty. [61] However, this desire leaves international law in a cliff-hanger. Is this practice a necessity or liability?

b. Enforcement of Extraterritorial Jurisdiction: A Necessity or Liability?

Any Government can employ strongarm laws to domestically regulate local internet providers, intermediaries, and users. [62] However, as data sharing transcends across borders, there is a compelling need to expand the scope of invoking extraterritorial jurisdiction. Notably, states that allow GDPR to have territory in their space may not consider PDPB's extraterritorial jurisdiction due to the colonial history. Therefore, India may still suffer the perception of being either a poor country or a fast developing nation that other states may not appreciate. This is

---

53 Id.

54 Article 3(2) — This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law. 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

55 Ricky Leung, "Navigating the GDPR's Extraterritorial Applicability to Processors: A Perspective from the Non-EU Cloud Service Provider" (August 2018), http://dx.doi.org/10.13140/RG.2.2.32800.43529.

56 Adèle Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation," *Journal of Intellectual Property, Information Technology and E-Commerce Law* 9, no. 2 (2018), https://www.jipitec.eu/issues/jipitec-9-2-2018/4723.

57 "Law in Singapore", DLA Piper, accessed April 12, 2021, https://www.dlapiperdataprotection.com/index.html?t=law&c=SG.

58 "Privacy Act 1988, Section 5B, paragraph 3(b)", accessed April 12, 2021, https://www.legislation.gov.au/.

59 Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. ("FCPA").

60 Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, 2006), 111.

61 Svantesson, "The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses."

62 Goldsmith and Wu, *Who Controls the Internet? Illusions of a Borderless World*, 159.

where the PDPB's §37 [63] may prove instrumental, as delisting certain foreign data fiduciaries may pave way to a more diplomatic understanding with such jurisdictions and consequently earn the faith to claim extraterritorial jurisdiction for other data fiduciaries. However, the PDPB lacks a provision that is similar to Article 58(1)[64] of the GDPR, which institutes a supervisory authority to command the functions of another jurisdiction operator. Notably, the LGPD also lacks such a provision.

The extraterritoriality principle in DPLs only intends to achieve measures to protect the sovereignty of stakeholder states. Unlike international criminal jurisdiction cases, there is no real claim for land or air present. Therefore, diplomacy may be an easy yet affordable tool to establish cooperation among jurisdictions. "The consent of the foreign state must be obtained" [65]. Even China enumerates this principle,[66] and Spain and Germany have already settled on an understanding to transfer personal data [67]. Therefore, this is not an impossible task anymore; only administrative and judicial cooperation is required.[68]

c. Self-Regulation and Safeguarding Data by Corporations Around the World

Diplomatic relations always seek a direct means of enforcement and the success quotient relies on lots of political, socio-economic factors.[69] However, there are other factors that a corporation may consider and, as a result, the state will consider before condescending to extraterritorial agreements with the other states.[70] Reputation is a key stake that corporations would hesitate to risk as a result of non-compliance. Therefore, the overarching coverage of DPLs on privacy aspects may require corporations to comply with such regulations.[71] Google testified this truth in the *Google v. Spain* case.[72] Likewise, when Facebook attempted to function parallel but not exactly complying with the GDPR, its reputation was thrown to a borderline contempt from the public. This forced Facebook to comply with the GDPR later.[73] However, the threat to reputation may

---

[63] §37 – Power of Central Government to Exempt Certain Data Processors — The Central Government may, by notification, exempt from the application of this Act, the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.

[64] Article 58 of the GDPR — Powers of the Supervisory Authority.

[65] Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2)* (International Journal of Law and Information Technology, Oxford University Press, 2010), 232.

[66] Article 277 of China's Personal Information Protection Law —

[67] See Commission Decision 2001/497 of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, 2001 O.J. (L 181/19)

[68] Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation."

[69] Cedric Ryngaert, "The Concept of Jurisdiction in International Law," Utrecht University, n.d., https://unijuris.sites.uu.nl/wp-content/uploads/sites/9/2014/12/The-Concept-of-Jurisdiction-in-International-Law.pdf.

[70] Nicole Lindsey, "Understanding the GDPR Cost of Continuous Compliance," CPO Magazine, 2019, accessed April 13, 2021, https://www.cpomagazine.com/data-protection/understanding-the-gdpr-cost-of-continuous-compliance/.

[71] "15 Unexpected Consequences of GDPR," Forbes Technology Council, n.d., accessed April 13, 2021, https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequencesofgdpr/#1ff037ae94ad.

[72] *Google v. Spain*, Court of Justice of the European Union [CJEU], ILEC 060 (CJEU 2014).

[73] David Ingram and Joseph Menn, "Exclusive: Facebook CEO Stops Short of Extending European Privacy Globally," reuters.com, n.d., accessed April 13, 2021, https://www.reuters.com/article/us-facebook-ceo-

not be grave for small-scale data fiduciaries.[74] This will further encourage corporations to self-comply with the DPL's ecosystem. This is a noteworthy model of claiming extraterritorial jurisdiction without the state initiating any processes.[75] The self-regulations feed on a company's fear of losing reputation. If the self-compliance program is popularized on the internet and among users, then corporations will be forced to comply with the regulations.[76]

GDPR's Chapter V regulates data transfer to third countries[77] to ensure the primary safeguards of the data of data principals of one state when they interact with entities belonging to another state.[78] On the other hand, the PDPB lacks this overarching extraterritorial concept in its basic architecture. Regulating data transfer may effectively protect a principal's personal data from being extradited by website cookies or even vendors/sellers from other countries.[79] This contradicts the full-compliance function of Article 3. Chapter V fills the miniscule voids left by the wide scoped Article 3.[80] Arguably, as the usage of the internet becomes prevalent, so is the threat of losing personal data.[81] Therefore, regulating data transfer may also result in personal data being leaked through unnoticeable channels to third countries[82].

IV. Conclusion and Recommendations

As the entire global users' daily routine relies on the internet and digital communication channels, there is an urgent need for various international agreements to be ratified to promote peace and cordial relations among states. Since internet and technology transcend through space and borders, the understanding and conceptualization of the jurisdictions of land, water, and space also need to be broadened and equally progressive. The thought process of sources of international law is still the ideals formulated in the industrial era and since technology and internet have caused a paradigm shift in the way communication and interactions occur, international laws should also be updated to meet contemporary needs.

In light of all these, the extraterritorial scope of DPLs cannot be exempted. The ideal trend should be to widen DPLs' scope of jurisdiction to make the impending concept of jurisdictions future-proof. States should formulate laws that safeguard their sovereignty. The response to this stimulus should also be reflected on other states whose sovereignty would be at stake as a result of

privacy-exclusive-idUSKCN1HA2M1. Exclusive: Facebook CEO stops short of extending European privacy globally | Reuters.

74 Jeffrey Batt, "Reputational Risk and the GDPR: What's at Stake and How to Handle I," Brink News, 2018, accessed April 13, 2021, https://www.brinknews.com/reputational-risk-and-the-gdpr-whats-at-stake-and-how-to-handle-it/.

75 Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2)*.

76 Svantesson, "The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses."

77 GDPR Chapter V — Transfers of personal data to third countries or international organisations.

78 Leung, "Navigating the GDPR's Extraterritorial Applicability to Processors: A Perspective from the Non-EU Cloud Service Provider."

79 Svantesson, "The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses."

80 Svantesson.

81 Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation."

82 Indriana Pramesti and Arie Afriansyah, "Extraterritoriality of Data Protection: GDPR and Its Possible Enforcement in Indonesia," in *Advances in Economics Business and Management Research, 3rd INCLAVE 2019, Volume 130* (Atlantis Press, 2019).

the former. With the PDPB, GDPR, and LGPD having a limited jurisdictional nexus, it is difficult to formulate successful international laws. However, the findings of the current study reveal that with the gritty construction of the GDPR, EU states have managed to defend their sovereignty as well as their subjects' interests without compromise. India should also ardently promote its interests through data protection tools that piece across jurisdictions through space. The PDPB is the best tool that India has to achieve what the EU did. Since the PDPB is before the JPC, the road may still lead to a successful future of the nation.

REFERENCES

Azzi, Adèle. "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation." *Journal of Intellectual Property, Information Technology and E-Commerce Law* 9, no. 2 (2018). https://www.jipitec.eu/issues/jipitec-9-2-2018/4723.

Batt, Jeffrey. "Reputational Risk and the GDPR: What's at Stake and How to Handle I." Brink News, 2018. https://www.brinknews.com/reputational-risk-and-the-gdpr-whats-at-stake-and-how-to-handle-it/.

Bioni, Bruno. R. "A Produção Normativa a Respeito Da Privacidade Na Economia Da Informação e Do Livre Fluxo Informacional Transfronteiriço." In *Direitos e Novas Tecnologias: XXIII National Meeting of Conpedi, 1*, 59–82, 2014. https://brunobioni.com.br/wp-content/uploads/2020/02/internet-sectoral-overview-xi-2-privacy-7-11.pdf.

Bowett, D. W. "Jurisdiction: Changing Patterns of Authority Over Activities and Resources." *BYIL* 53, no.1 (1982).

China's Personal Information Protection Law.

Commission Decision 2001/497 of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, 2001 O.J. (L 181/19).

Crawford, James. *Brownlie's Principles of Public International Law*. 8th edn. OUP, 2012.

Forbes Technology Council. "15 Unexpected Consequences of GDPR." n.d. https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequencesofgdpr/#1ff037ae94ad.

Foreign Corrupt Practices Act of 1977 of the United States of America.

Francke, Glory. "Time to Update Your Privacy Statement For GDPR." *Law 360*, n.d.

Goldsmith, Jack, and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press, 2006.

Google v. Spain, Court of Justice of the European Union [CJEU], ILEC 060 (CJEU 2014).

Ingram, David, and Joseph Menn. "Exclusive: Facebook CEO Stops Short of Extending European Privacy Globally." n.d. https://www.reuters.com/article/us-facebook-ceo-privacy-exclusive-idUSKCN1HA2M1.

International Court of Justice.

International Covenant on Civil and Political Rights.

Kuner, Christopher. *Data Protection Law and International Jurisdiction on the Internet (Part 2)*. International Journal of Law and Information Technology, Oxford University Press, 2010.

Lei Geral de Proteção de Dados.

Leung, Ricky. "Navigating the GDPR's Extraterritorial Applicability to Processors: A Perspective from the Non-EU Cloud Service Provider." (2018). http://dx.doi.org/10.13140/RG.2.2.32800.43529.

Lindsey, Nicole. "Understanding the GDPR Cost of Continuous Compliance." CPO Magazine, 2019. https://www.cpomagazine.com/data-protection/understanding-the-gdpr-cost-of-continuous-compliance/.

Maillart, Jean-Baptiste. "The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime." *ERA Forum* 19 (2019). https://doi.org/10.1007/s12027-018-0527-2.

Milanovic, Marko. *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy*. OUP, 2011.

Nottebohm Case (Liechtenstein v. Guatemala); Second Phase, International Court of Justice (ICJ).

Perrone, Christian. "Privacy and Data Protection - From Europe To Brazil," n.d. https://doi.org/http://dx.doi.org/10.17768/pbl.y6.n9-10.

Personal Data Protection Act, 2012 of Singapore.

Privacy Act 1988 of Australia

Pramesti, Indriana, and Arie Afriansyah. "Extraterritoriality of Data Protection: GDPR and Its Possible Enforcement in Indonesia." In *Advances in Economics Business and Management Research, 3rd INCLAVE 2019, Volume 130*. Atlantis Press, 2019.

Ryngaert, Cedric. "The Concept of Jurisdiction in International Law." Utrecht University, n.d. https://unijuris.sites.uu.nl/wp-content/uploads/sites/9/2014/12/The-Concept-of-Jurisdiction-in-International-Law.pdf.

SS 'Lotus' (France v Turkey) (1927) PCIJ Ser A, No 10.

Svantesson, Dan Jerker B. "The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses." *Stanford Journal of International Law* 50, no. 1 (2014): 53–102.

Internetsociety.org. "The Internet and Extraterritorial Effects of Laws Internet Society Concept Note." Accessed April 11, 2021. https://www.internetsociety.org/wpcontent/uploads/2018/10/The-Internet-and-extraterritorial-application-of-laws-EN.pdf.

The United States of America's Helms Burton Act.

The Personal Data Protection Bill, 2019.

The General Data Protection Regulation 2016/679.

The General Personal Data Protection Law 13709/2018.

The Recommendations of the Justice Srikrishna Report.

UK vs. Norway (North Atlantic Fisheries Case), [1951] ICJ Rep.116.

Universal Declaration of Human Rights.Vienna Convention on Diplomatic Relations 1961, Done at Vienna on 18 April 1961. Entered into force on 24 April 1964. United Nations, Treaty Series, vol. 500.

Walia, Harish, and Supratim Chakraborty. "Indian Data Protection Law." iclg.com, n.d. Accessed April 11, 2021. https://iclg.com/practice-areas/data-protection-laws-and-regulations/india.