No. 28 (2) 2020 IIUMLJ 531 - 565

EXTRATERRITORIAL APPLICATION OF THE EU GENERAL DATA PROTECTION REGULATION: AN INTERNATIONAL LAW PERSPECTIVE

Md. Toriqul Islam*

Mohammad Ershadul Karim**

ABSTRACT

The General Data Protection Regulation (the GDPR) of the European Union (EU) emerges as a hot-button issue in contemporary global politics, policies, and business. Based on an omnibus legal substance, extensive extraterritorial scope and influential market powers, it appears as a standard for global data protection regulations as can be witnessed by the growing tendency of adopting, or adjusting relevant national laws following the instrument across the globe. Under Article 3, of the GDPR applies against any data controller or processor within and outside the EU, who process the personal data of EU residents. Therefore, the long arm of the GDPR is extended to cover the whole world, including Malaysia. This gives rise to tension worldwide, as non-compliance thereof leads to severe fines of up to €20 million or 4% of annual turnover. This is not a hypothetical possibility, rather a reality, as a huge amount of fines are already imposed on many foreign companies, such as Google, Facebook, Uber, and Equifax to name a few. Such a scenario, due to the existence of state sovereignty principles under international law, has made the researchers around the world curious about some questions, why does the EU adopt an instrument having the extraterritorial application; whether the extraterritorial scope is legitimate under normative international law; how the provisions of this instrument can be enforced, and how these are justified. This article attempts to search for answers to those questions by analyzing the relevant rules and norms of international law and the techniques of the EU employed. The article concludes with the findings that the extraterritorial scope of the GDPR is justified under international law in a changed global context. The findings of

* PhD Candidate, Faculty of Law, University of Malaya; Assistant Professor, Bangladesh University of Business and Technology (BUBT). Email: toriqul@siswa.um.edu.my.

** Senior Lecturer at Faculty of Law, University of Malaya. Email: ershadulkarim@um.edu.my.

[Received: 2 October 2019, Accepted: 17 November 2020, Published: 28 December 2020]

this article will enlighten the relevant stakeholders, including Malaysian policymakers and business entities, to realise the theoretical aspects of inclusion of the extraterritorial feature of the GDPR, and this understanding may facilitate them to map their future strategies.

Keywords: extraterritorial jurisdiction, state sovereignty, legality of extraterritorial scope, principles of international law, rationales of the EU.

APLIKASI ESKTRATERITORIAL DALAM PERATURAN PERLINDUNGAN DATA UMUM OLEH KESATUAN EROPAH: SATU PERSPEKTIF UNDANG-UNDANG ANTARABANGSA

ABSTRAK

Peraturan Perlindungan Data Umum (GDPR) oleh Kesatuan Eropah (EU) muncul sebagai isu panas dalam politik global kontemporari, polisi dan perniagaan. Berdasarkan peranan undang-undang omnibus, skop esktrateritorial yang luas dan pengaruh kuasa pasaran, ianya dilihat sebagai standard global untuk peraturan perlindungan data seperti yang boleh disaksikan melalui kecenderungan terhadap penerimaan atau penyesuaian undang-undang nasional yang berkaitan agar selaras dengan instrumen itu di seluruh dunia. Dalam Artikel 3 GDPR, ianya terpakai terhadap pengawal data dan pemproses data di dalam atau di luar EU, sesiapa yang memproses data peribadi rakyat EU. Oleh itu, aplikasi GDPR dipanjangkan ke seluruh dunia termasuk Malaysia. Ini memberikan tekanan keatas seluruh dunia, kerana ketidakpatuhan akan membawa kepada denda sebanyak €20juta atau 4 peratus daripada perolehan tahunan. Ini bukanlah satu kemungkinan tetapi kenyataan kerana jumlah denda yang besar telah dikenakan terhadap banyak syarikat asing gergasi seperti Google, Facebook, Uber dan Equifax. Kerana itu, disebabkan oleh kewujudan prinsip negara berdaulat di bawah undang-undang antarabangsa telah membuatkan penyelidik di seluruh dunia tertanya beberapa soalan, kenapa EU menerima satu instrumen yang mempunyai aplikasi esktrteritorial; adakah skop ekstrteritorial ini sah di bawah undang-undang antarabangsa normatif; bagaimana peruntukan-peruntukan dalam instrumen ini boleh di laksanakan, dan sejauh mana ianya wajar. Makalah ini cuba untuk mencari jawapan kepada soalan-soalan tersebut dengan menganalisis peratuan yang relevan dan norma undang-undang

antarabangsa dan teknik-teknik yang digunakan oleh EU. Artikel ini menyimpulkan bahawa penemuan skop esktrateritorial GDPR adalah wajar di bawah undang-undang antarabangsa dalam konteks global yang sudah berubah. Penemuan di dalam makalah ini akan memberikan pencerahan kepada pihak berkepentingan yang relevan termasuklah penggubal dasar Malaysia dan entiti perniagaan untuk menyedari aspek teori dalam kemasukan aspek esktrateritorial GDPR dan kefahaman ini akan membantu mereka untuk mencorakkan strategi di masa hadapan.

Kata kunci: bidang kuasa extraterritorial, negara berdaulat, skop esktraterritorial sah, prinsip undang-undang antarabangsa, rasional Kesatuan Eropah.

INTRODUCTION

Personal data is considered as the currency and oil of the internet in this digital era, as without the use of personal data, diversified and desired use of the internet cannot be ensured. Before commencement of the GDPR[1] in May 2018, EU Member States would enforce their data privacy laws according to EU 'Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data' (Directive 95/46/EC).[2] The Directive 95/46/EC often caused a patchwork in diverse privacy protection mechanisms in the region enabling multi-national companies to pick and rely on a jurisdiction watching enforcement mechanism.[3]

---

1 European Parliament and Council, "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," (the GDPR) *Official Journal of the European Union OJL* 119, 4.5.2016 (May 25, 2018).

2 European Parliament and Council, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," (Directive 95/46/EC) *Official Journal of the EC* 23, no. 6 (1995).

3 Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 1)," *International Journal of Law and Information Technology* 18, no. 2 (2010): 176-93.

Therefore, the same degree of protection in respect of privacy and personal data within the EU could not be ensured through that Directive. Such a scenario forced EU regulators to introduce an instrument harmonizing all data privacy laws of the region by extending the territorial scope of the previous Directive. Thus, the provision of extraterritorial jurisdiction was included in Article 3 (2) of the GDPR to provide better protection for the personal data of EU citizens.

Nonetheless, this stand of the GDPR raises several inevitable questions, such as what are the implications of the GDPR? Why should the GDPR be recognized and diffused globally? Why does the GDPR incorporate provisions of extraterritorial jurisdiction? Which norms of international law legitimate the inclusion of such provisions? How can the EU authorities apply their regulations outside the region? Keeping all these questions in mind, this article attempts to review the global recognition and diffusion, aspirations, legal bases, challenges, and global implications of extraterritorial application of the GDPR.

This article begins with an analysis of the implications of the GDPR, followed by reasons for global acceptance and the diffusion thereof. Later, it searches for answers as to why the GDPR aspire in adopting the extraterritorial reach, and whether there is any legality for this extraterritorial scope. Subsequently, it focuses on enforcement mechanisms of the GDPR in instances involving extraterritorial jurisdiction, and finally, the article analyses the justification of incorporating extraterritorial jurisdiction of the GDPR. The findings of this article may assist relevant stakeholders, including Malaysian policymakers and business entities, in understanding the theoretical aspects of inclusion of such provision of the GDPR and such an understanding may facilitate them to map their future strategies.

IMPLICATIONS OF THE GDPR

Due to overarching provisions, exclusive market power and extensive extraterritorial scope, the GDPR appears as the global data privacy standard, the implications of which are undeniable from any part of the globe, and Malaysia is not an exception. Nowadays, it has tremendous effects on how data is managed within and outside the EU and plays a significant role in shaping privacy

legislation across the world. Recently, the UN Special Rapporteur on 'the right to privacy', for example, remarks that:

> The protection of personal information online should be a priority with the adoption of provisions equivalent or superior to the GDPR, for countries those are not parties to the Regulation.[4]

Consequently, many countries in Europe other than the EU Member States, e.g., Iceland, Liechtenstein, Norway and Switzerland, changed their data protection laws in harmony with the GDPR.[5] Even other non-European countries such as numerous countries from Africa, Asia, the Caribbean and Latin America are either enacting new data privacy laws or amending previous laws to ensure that the domestic law is in harmony with the GDPR.[6] Lawyers working with *Ius Laboris* have identified that there are at least 24 countries outside the EU in which there exist GDPR-related legal developments, decisions or trends of harmonization.[7]

Rustad and Koenig surveyed the global data privacy standard and concluded that the net impact of the GDPR is two-folded, e.g., (1) transatlantic privacy convergence, and (2) rapid evolution as the global data privacy standard.[8] To resonate with their findings, it can be revealed that numerous countries across the globe, including many states of the United States of America (US), and most US-based data

---

4 Cannataci J, *Report of the Special Rapporteur on the Right to Privacy*, October 17, 2019, A/HRC/40/63, para 107: 16, https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08.

5 Nymity, "Happy Birthday GDPR. At One Year on, What have We Learned?," Lexology, last modified June 5, 2019, https://www.lexology.com/library/detail.aspx?g=649cd552-7853-4abc-81c6-37af2c8dd415.

6 Graham Greenleaf and Bertil Cottier, "Data Privacy Laws and Bills: Growth in Africa, GDPR Influence," *(April 12, 2018)* 152 (2018): 5.

7 "The Impact of the GDPR Outside the EU," Ius Laboris: Global HR Lawyers, last modified September 17, 2019, https://theword.iuslaboris.com/hrlaw/whats-new/the-impact-of-the-the GDPR-outside-the-eu.

8 Ibid, 365-366.

processors have been introducing, or have already introduced policies in conformity with the GDPR.[9] Their findings also revealed that the African data privacy standard is usually undeveloped and the approach to data privacy legislation in Asian countries is mostly leaning toward compliance with the GDPR.[10] Finally, they conclude, the emergence of a the GDPR-styled privacy standard is found not only in the 'First World' but also in the 'Second World' and the 'Third World' countries.[11]

Based on the above literature, we can conclude that the GDPR appears as the model for global data privacy laws and accordingly, followed worldwide. Thus, Giovanni Buttarelli refers to the GDPR as a clarion call for a unique global data privacy gold standard.[12] Probably, considering this, Malaysia plans to amend the Personal Data Protection Act, 2010 (PDPA)[13] by using the GDPR as one of the guiding stars. In the words of the former Minister of Communications and Multimedia:

> We had identified there are gaps within the Act and its position when compared to personal data protection legislation in ASEAN member nations, Japan, South Korea and also the European Union's (EU) General Data Protection Regulation (the GDPR).[14]

Upon identification of some substantial gaps in the PDPA, subsequently, the Ministry issued a document titled, 'Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010' asking comments from people on 22 issues (14-

---

9 Ibid, 366.

10 Ibid, 449.

11 Ibid, 365-366.

12 Giovanni Buttarelli, "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard," *International Data Privacy Law* 6, no. 2 (2016): 77.

13 Personal Data Protection Act 2010, (PDPA) Malaysia, Act no. 709, as at 15 June 2016.

14 "Minister: Govt to Consult Public on Amendments to Personal Data Protection Law," *malaymail*, last modified February 12, 2020) https://www.malaymail.com/news/malaysia/2020/02/12/minister-govt-to-consult-public-on-amendments-to-personal-data-protection-l/1836984.

28 February 2020) encompassing the PDPA, which is under consideration.[15] Notwithstanding the above, there may be some other reasons why the GDPR has been recognized and globally diffused as a standard for global data protection laws. In the subsequent section, we would search for some of those reasons.

REASONS FOR GLOBAL ACCEPTANCE AND DIFFUSION OF GDPR

Many authors attempt to find out reasons behind the worldwide recognition and diffusion of the GDPR, and among them, the works of Paul M. Schwartz, Anu Bradford, Jack Goldsmith and Tim Wu are worth discussing. According to them, the GDPR has received an unprecedented extension due to three factors, such as (1) an omnibus legal substance,[16] (2) the 'Brussel's Effect',[17] and (3) an influential market power.[18] In addition to the above three factors, the adequacy of the decisions of the European Commission (EC) is also a significant contributing factor to the global recognition and acceptance of the GDPR. Let us examine all these four additional factors.

1. An omnibus legal substance

In searching for reasons for global recognition and diffusion of the GDPR, Schwartz identifies that two overarching factors contribute to the global diffusion of the EU data protection law, such as (a) legal substance, and (b) omnibus legislative approach.[19] To him, due to contextual relevance and highness, EU initiatives toward data

---

15 Ministry of Communications and Multimedia, *Review of Personal Data Protection Act 2010* (Public Consultation Paper, No 01/2020, February 2020), accessed April 14, 2020, https://www.pdp.gov.my/jpdpv2/assets/2020/02/Public-Consultation-Paper-on-Review-of-Act-709_V4.pdf.

16 Paul M Schwartz, "Global Data Privacy: The Eu Way," *New York University Law Review* 94 (2019): 4.

17 Anu Bradford, "The Brussels Effect," *Northwestern University Law Review* 107 (2012): 1.

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

19 Schwartz, "Global Data Privacy," 1.

protection has always been the subject of legal conversations of the world's leading institutions and individuals, and this has eventually led to the transplantation of the GDPR into other privacy protection mechanisms in the world.[20] The EU relied on its highly accessible omnibus regulations which include both public and private sectors, and therefore, demonstrated them for other countries to foster. Even though he claims, the EU did not devise this model having international aspirations in mind, rather, it was prepared to harmonize the data protection regime among its Member States, which started to face problems since the 1970s.[21]

2. The 'Brussel's' effect

Bradford, on the other hand, speculates that the dominance of the EU law is an output of the 'Brussel's Effect'.[22] This circumstance happens whenever an individual nation attempts to exteriorize its legal norms beyond its boundary by market power, leading to the globalization of standards.[23] Furthermore, private bodies outside the EU progressively stressed on the adherence to EU law, as Bradford says, even though the EU governs only its domestic market, the international companies have always had motivations to deal with their commodities worldwide by applying a single rule.[24] The statement of UN Special Rapporteur on 'the right to privacy', 2018, is worth mentioning here, which reveals that:

> The GDPR's influence is not exerted only through local legislative enactments or its extraterritorial application. Companies outside Europe, Microsoft being the most prominent example, are voluntarily adopting 'the GDPR compliance' across their whole business operations irrespective of a legal obligation to do so.[25]

Sometimes, export-oriented industries regulate their business following the EU model and lobby with the policymakers of their States to enact laws conforming to the EU standards in order to obtain

---

20 Ibid, 4.
21 Ibid.
22 Bradford, "The Brussels Effect," 38.
23 Ibid.
24 Ibid, 6.
25 Cannataci J, *Report of the Special Rapporteur on the Right to Privacy*, October 17, 2018, A/73/4571, https://undocs.org/A/73/438.

competitive benefits in their own country against their non-export-oriented counterparts.[26] For example, after the GDPR is adopted in the EU, numerous technology giants, including Google, Facebook, Microsoft and Apple urged the Federal Government of the USA to enact a federal data privacy legislation similar to the GDPR.[27] Needless to say that California Consumer Privacy Act (CCPA), 2018 is nothing but the feedback of such kind of appeal. Moreover, businesses' de facto adaptation toward EU law lays down the foundation for lawmakers' de jure enforcement of these laws, which Bradford calls as 'de jure Brussels Effect'.[28]

3. The influential market power

Operating as a union of 27 countries, the EU is the top single market in the world and one of the three largest leading actors in global trade together with the USA and China.[29] Moreover, the EU appears as one of the largest trading partners for almost all nations of the world, contributing 22% in global nominal GDP.[30] Besides that, the EU retains both coercive and persuasive tools and means to shape international affairs.[31] With this influential market power, arguably, the roles, laws and policies of the EU inevitably affects the whole world, including Malaysia.

To explain the matter, Goldsmith and Wu remarks, EU's privacy regulations are the fourth type of global legislation. They are neither a convention nor enforceable architecture, like ICANN; not a

---

26 Bradford, "The Brussels Effect," 6.

27 Sam Pfeifle, "US Federal Privacy Law? Apple, Google, Facebook, Microsoft All Hope So," The Privacy Advisor, IAPP, last modified, October 25, 2018, https://iapp.org/news/a/us-federal-privacy-law-apple-google-facebook-microsoft-all-hope-so/#.

28 Ibid, 8.

29 "The Economy," European Union, accessed April 15, 2020, https://europa.eu/european-union/about-eu/figures/economy_en.

30 "Economy of the European Union," Wikipedia, last modified April 14, 2020, https://en.wikipedia.org/wiki/Economy_of_the_European_Union#cite_note-26.

31 Damro Chad "Market Power Europe," *Journal of European Public Policy* 19, no. 5 (2012): 682-699.

WTO-regulated trade dispute, like online gambling; but rather, global regulations arising out of EU's noteworthy concern for resident's privacy and unique combination of EU's immense market power.[32]

Based on this market power, the GDPR may have considerable impacts on the Malaysian business, legal and policy affairs, as the EU is one of the largest trading partners of Malaysia.[33] In terms of the GDP, Malaysia, the third biggest economy in ASEAN, is the third major business partner of EU in the region.[34] After China and Singapore, the EU is Malaysia's third major business partner, sharing a market of 11.6% of its total trade.[35] Malaysia became EU's twenty third global biggest business partner in goods, accordingly, sharing an amount of €39.8 billion in 2018.[36] Therefore, the implications of the GDPR cannot be ignored in the context of Malaysia, rather the GDPR may play major roles in shaping her policies, politics and businesses, including personal data protection regime.

4. Adequacy decisions

There has been an immense influence of adequacy decisions of the EC all over the world, including Malaysia. The adequacy decision is the power of the EC to assess whether a specific country, territory, or international organization outside the EU offers an adequate level of protection for personal data.[37] Based on the adequacy decisions, EU restricts transfers of personal data of EU residents outside European

---

32 Wu and Goldsmith, *Who Controls the Internet?* 176.

33 Abu Bakar Munir and Yasin Siti Hajar Mohd. *Personal Data Protection in Malaysia: Law and Practice* (Sweet & Maxwell, 2010), 213.

34 "Countries and Regions" European Commission, accessed April 15, 2020, https://ec.europa.eu/trade/policy/countries-and-regions/countries/malaysia/.

35 Ibid.

36 Ibid.

37 de Carvalho, Duque, and Sara Leonor, "Key GDPR Elements in Adequacy Findings of Countries that have Ratified Convention 108," *European Data Protection Law Review* 5 (2019): 54; "Data Protection if There's No Brexit Deal," ICO: Information Commissioner's Office, accessed April 15, 2020, https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal-3/the-the GDPR/international-data-transfers/.

Economic Area (EEA), assuming that EU citizens would not get adequate protection of the GDPR in respect of their personal data.[38]

As per the provision of Article 45 of the GDPR, if data privacy law of a particular country does not comply with the GDPR, the EC can declare that they are deemed to have an inadequate privacy regime. Consequently, most global trading partners of the EU are trying to obtain adequacy decisions from the EC to boost up their trade relations with the EU. For example, currently, Andorra, Argentina, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay have obtained the complete adequacy decision, and partial findings of adequacy were granted for Canada and the USA.[39] Recently, EC is working on adequacy decision about South Korea.[40]Unfortunately, Malaysia is neither on the list nor in any consideration.

Given that fact, there remains an obvious question, whether there are ways of processing or transferring data from the EU to Malaysia and vice-versa when Malaysia does not fulfil adequacy requirements. The personal data can still be transferred to Malaysia subject to the fulfilment of appropriate safeguards. Article 46 of the GDPR, for example, renders that in the absence of a decision (adequacy decision) under Article 45 (3), personal data may also be transferred to third countries or transnational institutions only when controllers or processors have ensured three things for data subjects, e.g., (a) appropriate safeguards; (b) enforceable data subject rights and (c) effective legal remedies.

In this regard, the remarks of Professor Munir is worth mentioning. To him, it was hoped that the PDPA would promote the free flow of data in trade and other joint initiatives. Nonetheless, if Malaysia cannot satisfy the adequacy test, and both EU and

---

38 "International Transfers," ICO: Information Commissioner's Office, accessed April 15, 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-the GDPR/international-transfers#eea-states. Of course, in the case of no adequacy decision, personal data of the EU can still be transferred under Article 46 and 49 of the GDPR.

39 "Adequacy Decisions," European Commission, accessed September 2, 2019, https://ec.europa.eu/info/law/lawtopic/dataprotection /international- dimension-data-protection/adequacy-decisions_en.

40 "International Transfers," ICO.

Malaysian businesses are to depend on further contracts for data transfer, then the PDPA is said to be a missed opportunity.[41] It is noteworthy that there remained considerable gaps regarding extraterritorial reach in the previous EU Directive 95/46/EC as discussed earlier in the introduction of this article. Therefore, the issue requires to have some details on it, and to this end, the following analysis has been offered.

REASONS FOR INCORPORATING THE PROVISION OF EXTRATERRITORIAL JURISDICTION IN THE GDPR

The protection of data privacy is becoming complicated day by day because of numerous reasons, e.g., globalization in communication; growing attention on data processing by the Government and non-Government actors; deliberate data sharing in social media; commercialisation of data; utilisation of cloud computing, and above all, valuing privacy as one of the basic human rights.[42] Consequently, though once the phrases 'data controller', 'data subject' and the 'data-processing mechanisms' usually meant and explained in views of national legislation only, they are now defined in a global context, and this new landscape has contributed to widening the territorial scope of the GDPR.

In particular, the GDPR aspires to extend its territorial application because of the following limitations of Directive 95/46/EC: (1) The Directive had limited territorial scope, as a result, data protection rules could be applied only to controllers and establishments that physically existed in the EU; for multiple establishments of the same controller, each of establishments could apply laws of the concerned Member States.[43] (2) It could apply against overseas controllers on two grounds only; firstly, where national laws of any Member State would apply on that controller under public international law, and secondly, where, other than transit purpose, such overseas controllers set establishments in EU territory

41 Munir and Yasin, *Personal Data Protection in Malaysia*, 224.

42 Christopher Kuner, Fred H Cate, Christopher Millard, and Dan Jerker B Svantesson, "The extraterritoriality of data privacy laws—An Explosive Issue Yet to Detonate," *International Data Privacy Law* 3, no. 3 (2013): 147.

43 Directive, "95/46/EC," Article 4 (1) (a).

for processing personal data of EU residents by using any equipment, automated or otherwise.[44] (3) The Directive was to depend much on the interpretation and intervention of the court in question, which EU authorities did not like.

Over time, technological advancements equipped companies with opportunities of processing data from a remote place which could easily despoil territorial scope of Directive except by an intervention of the European Court of Justice (ECJ). The famous *Google Spain*[45] case demonstrated that data processing activities conducted by US-based Google Inc. had become profitable through operations of EU establishment, Google Spain. Accordingly, the commercial ties between the US controller i.e. Google Inc. and the EU establishment i.e. Google Spain would deem as data processing by the EU establishment.[46]

However, the EU aspires not to receive such interpretation and intervention of the Court evermore, and thus, took initiatives to incorporate provisions of extraterritorial application in the GDPR.[47] Hence, the precise intention behind the inclusion of provision on the extraterritorial application of the GDPR was to ensure the rights of data subjects and to secure more certainty for both data subjects and controllers.[48]

Nonetheless, the inclusion of the extraterritorial jurisdiction in the GDPR and its application, challenge the long-standing State's sovereignty principles, which need to be clarified. In the following

---

44 Ibid, Article 4 (1) (b) (c).

45 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 2014 O.J. C. 212 (2014).

46 Ibid.

47 Adele Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law.* 9 (2018): 128.

48 Council of the European Union, "Draft Statement of the Council's Reasons 3 (providing the Council's reasons for proposing the GDPR and repealing the Directive) [hereinafter Council's Reasons]," 5419/16 ADD 1 REV 1 DGD 2C VH/Np" 2016, no. March (2016): 1–36. See also, Wimmer, Kurt. "The Long Arm of the European Privacy Regulator: Does the New EUGDPR Reach US Media Companies?" *Communications* 17 (2017): 17.

section, we analyze how can the extraterritorial jurisdiction of the GDPR be adjusted with long-settled State's sovereignty principles.

STATE'S SOVEREIGNTY VERSUS EXTRA TERRITORIALITY OF JURISDICTION

The notion of 'jurisdiction' plays a pivotal role in the State-citizen relationship and exists by the application of the State's authority over its citizens. Traditionally, this heavy power of the State binds only persons, things or institutions existing within its territory.[49] Therefore, a State will outrage normative provisions of international law if it applies its sovereign authority on persons, things, and institutions beyond its territory. The precise logic against extraterritoriality proceeds with the assumption that all nations should be treated equally in terms of sovereignty, and none can be deprived of this right.[50]

In the context of both the scope and execution, 'sovereign immunity' refers to a legal norm, which is designed for the protection of the territorial integrity and dignity of nations.[51] This concept postulates that the judgement of a foreign court cannot be produced before any domestic court of another State in respect of any action or asset out of its explicit consent.[52] In principle, the contention advances with a common understanding that to force a State in

---

49 Council Regulation (EC) 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters," *Official Journal of the EC* 12, no. 1 (2001): Article 3(2) and Annex I.

50 For a general discussion, please see the territorial principle and effects doctrine under sub-heading 'customary international law' at Part VI. Please see also, the UN Charter, Article 2 (1) (4).

51 Manuel R. Garcia Mora, "The Doctrine of Sovereign Immunity of Foreign States and Its Recent Modifications," *Virginia Law Review* 42, no. 3 (1956): 336. See also, *Ulen & Co. v. Bank Gospodarstwa Krajowego*, 24 N.Y.S.2d 201, 261 App. Div. 1, 261 A.D. 1 (1940).

52 *United States of Mexico v. Rask*, 293 P. 108, 109 Cal. 497, 109 Cal. App. 497 (1930); *Republic of China v. National City Bank of New York*, 208 F.2d 627 (2d Cir. 1953); *Guaranty Trust Co. v. United States*, 304 U.S. 126, 58 S. Ct. 785, 82 L. Ed. 1224 (1938); *Principality of Monaco v. Mississippi*, 292 U.S. 313, 54 S. Ct. 745, 78 L. Ed. 1282 (1934). See also, Garcia Mora, "The Doctrine of Sovereign Immunity," 336.

admitting jurisdiction of another is simply a breach of the doctrine of equality of nations as recognised in the UN Charter. Article 2 of the United Nations Charter, for example, states:

> The organization is based on the principle of the sovereign equality of all its Members. All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or any other manner inconsistent with the purposes of the United Nations.

In his novel work, 'The Law of Nations', Emmerich de Vattel remarked that as per customary international law, every nation has the right to be free from the intervention of others, and can behave with its subjects in the manner and so long as it wishes, even though its behaviour would appear as ruthless to others.[53] In 1912, Oppenheim opined in his premier work, 'The Treatise on International Law' that State's territorial sovereignty or supremacy may normally expand or limit as much as it desires.[54] Nonetheless, he concluded that there is no right for States to expand its territorial reach over the activities of the foreigners in a logic that they have grown up by way of international law.[55]

The International Court of Justice (ICJ) firmly promotes jurisdictional immunities of States in the judgment of a recent

---

53 Emer de Vattel and Albert Geouffre de La Pradelle. *Le Droit Des Gens Ou Principes de la Loi Naturelle Appliqués À la Conduite Et Aux Affaires Des Nations Et Des Souverains: The Law of Nations or The Principles of Natural Law.* Carnegie Institution of Washington, 1758; Curran, Vivian Grosswald, "Extraterritoriality, Universal Jurisdiction, and the Challenge of *Kiobel v. Royal Dutch Petroleum Co*," *Maryland Journal of International Law* 28 (2013): 78. See also, De Vattel, Emer. *Le droit des gens ou principes de la loi naturelle: Translation of the edition of 1758, by Charles G. Fenwick, with an Introduction by Albert de Lapradelle*. no. 4. Carnegie Institution of Washington, 1916.

54 Lassa Oppenheim, "*International Law: A Treatise*, 2nd edn, Vol. I." (London: Longmans, Green, and Co, 1912). See also, Curran, "Extraterritoriality," 78.

55 Ibid, 204. See also, Curran, "Extraterritoriality," 78.

case, *Germany v. Italy: Greece intervening*.[56] In the proceeding, Germany insisted on three issues, such as (1) Italy infringed the principles of international law by carrying on civil suits in its domestic courts against Germany for the commission of war crimes by the German soldiers during the Second World War. (2) It outraged sovereign immunity of Germany initiating coercive measures against German's assets located in Italy, and (3) Italy breached Germany's sovereign immunity by claiming applicability of a judgment of Greek court delivered against Germany on the similar facts.[57]

Considering all issues in question, the ICJ pronounced its judgement favouring Germany arguing that Italy infringed principles of sovereign immunity in terms of both jurisdiction and enforcement. The ICJ further observed that the Italian courts violated Italy's international obligations by denial of sovereign immunity power of Germany. Additionally, the ICJ remarked that as per prevailing customary international law, no State is deprived of such immunity on the ground that once it violated international law of armed conflicts or international human rights law.[58]

The extraterritoriality refers to the application of jurisdictional claims of a State over actions beyond its territorial boundary;[59] though not a new conception, it receives considerable attention nowadays. Because of the world's transformation into a global village, increasing advancement in the ICT technologies, and growing dependence on online activities, many crimes and their particulars are committed in more than one jurisdiction. This transition extends traditional territorial jurisdictional limit under

---

56 *Germany v. Italy: Greece intervening*, 2012 I.C.J. Rep 99, 2012 I.C.J. 99 (2012).

57 Andrew Cannon, "The ICJ Firmly Upholds Principles of Sovereign Immunity in Its Recent Judgment in the Case of *Germany v Italy*," Lexology (Herbert Smith Freehills LLP), last modified March 8, 2012, https://www.lexology.com/library/detail.aspx?g=06b14d1c-afe3-48b6-8ce2-8bbfee4032d2.

58 "Jurisdictional Immunities of the State (*Germany v. Italy*: Greece intervening)," International Court of Justice, accessed September 1, 2019, https://www.icj-cij.org/en/case/143.

59 Senz Deborah, and Hilary Charlesworth, "Building Blocks: Australia's Response to Foreign Extraterritorial Legislation," *Melbourne Journal of International Law* 2, no. 1 (2001): 72.

public international law, and therefore, the assumption against extraterritoriality has been under fire.[60]

Mireille Delmas-Marty, the eminent French jurist, remarked that the split took place, not after the World War II or the Trials of Nuremberg, but after the World War I and the Versailles treaty, and this compelled to extradite Kaiser Wilhelm legally,[61] although the Dutch administration would deny provisions of extradition.[62] In 1927, the Permanent Court of International Justice asserted in a frequently cited *Lotus case* that, "....in respect of other cases, every nation is free to choose the principle that is the best suit with its condition".[63] Thus, the *Lotus case* upholds a State's power to apply its jurisdiction extraterritorially, demarcating distinctions between enforcing and prescribing.[64]

Subsequently, many international instruments, such as Brussels I Regulation,[65] Supplementary Protocol to the Hague Convention on the Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters,[66] and Preliminary Draft

---

60 Stephen J Adler, "Fighting Terrorism in the New Age: A Call for Extraterritorial Jurisdiction over Terrorists." *University of San Francisco Maritime Law Journal* 18 (2005): 171. See also, Walsh, Ryan. "Extraterritorial Confusion: The Complex Relationship between Bowman and Morrison and a Revised Approach to Extraterritoriality," *Valparaiso University Law Review* 47, no. 2 (2013): 629.

61 Delmas-Marty Mireille, "La responsabilité pénale en échec (prescription, amnistie, immunités)." *Antonio Cassese et Mireille Delmas-Marty (éds.), Juridictions nationales et crimes internationaux, PUF* 637 (2002). See also, Curran, "Extraterritoriality," 78.

62 Antonio Cassese, International *Law,* (Oxford University Press, 2008). See also, Curran, "Extraterritoriality," 78.

63 *FR v. Turk*, 1927 P.C.I.J. (ser. A) 10 (Supreme Court 1927).

64 Donald Francis Donovan and Anthea Roberts, "The Emerging Recognition of Universal Civil Jurisdiction," *American Journal of International Law* 100, no. 1 (2006): 142-163.

65 "Council Regulation," Article 3 (2) and Annex I. See also, Christopher Kuner, "Data Protection Law and International Jurisdiction on the InternetInternet (Part 2)," *International Journal of Law and Information Technology* 18, no. 3 (2010): 228.

66 "1144 UNTS 271," (concluded 1 February 1971, entered into force 20 August 1979), Article 4, http://hcch.e-

Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters drafted by the Hague Conference on Private International Law etc have recognised the issue of extraterritoriality.[67]

In this data-driven society, one must take into account the peculiar character of data, i.e., (1) data's intangibility, which does not mean that data remains nowhere,[68] rather anywhere, and even a part thereof may be available everywhere, and (2) data's accessibility without any physical proximity.[69] Particularly, the character of data's intangibility poses huge challenges to the theory of typical territorial State sovereignty and jurisdiction. Thus, Svantesson concluded that claims of extraterritorial jurisdiction are justified, and if a State does not expand its data protection mechanism to the behaviour of overseas actors, it would not be able to render adequate safeguard for its residents.[70]

Apart from sovereignty principles, there are numerous other mechanisms, which need to be tested for evaluating the legality of the extraterritorial scope of the GDPR, and to this end, we offer a wide range of such mechanisms below.

LEGALITY OF EXTRATERRITORIAL JURISDICTION

It is recognised that the more extensive than the territorial application is imposed by a State, the more logically others will reject to accept it.[71] Besides, there are numerous principles of international law either

vision.nl/index_en.php?act=conventions.text&cid=79. See also, Christopher Kuner, "Data Protection Law and International Jurisdiction on the InternetInternet (Part 2)," *International Journal of Law and Information Technology* 18, no. 3 (2010): 228.

67 "Special Commission," adopted on October 30, 1999, Article 18 (2), http://www.hcch.net/upload/wop/jdgmpd11.pdf. See also, Kuner, "Data Protection (Part 2)," 228.

68 Johnson, David R., and David Post, "Law and Borders--The Rise of Law in Cyberspace," *Stanford Law Review* 48 (1995): 1367.

69 Kristen E Eichensehr, "Data Extraterritoriality," *Texas Law Review* 95: 145.

70 Dan Jerker B Svantesson, "The Extraterritoriality of EU Data Privacy Law-Its Theoretical Justification and Its Practical Effect on US Businesses," *Stanford Journal of International Law* 50, no. 1 (2014): 55.

71 Ibid, 94.

to recognize or reject the extraterritorial jurisdiction of States. Meanwhile, under Article 3 (2), the GDPR applies against any foreign controllers, who process personal data of EU residents by offering goods or services, or monitor their behaviours. Non-compliance with this provision may lead to severe fines of up to €20 million or 4% of annual turnover, whichever is higher.[72] In such a context, before examining principles of international law, it is also essential to review the EU's logic concerning the extraterritorial scope of the GDPR.

1. The EU's visions and actions

It is always a concern for international law to determine the jurisdiction for a case that contains one or more foreign elements. In deciding such a case, protection of rights and interests of inhabitants, residents, businesses, and other stakeholders usually receive much attention. Thus, the penal laws of many countries incorporate provisions on a wide territorial application. For example, the combined reading of sections 3 and 4 of the Penal Code of Malaysia affirms that offences committed outside Malaysia can be prosecuted in Malaysia, and the law can be applied to try extraterritorial offences.[73] Howbeit, in the Working document 'Privacy on the Internet', Article 29 Data Protection Working Party pinpointed that trans-border approach in case of data privacy law is a usual phenomenon in international law.[74]

The EU's stand in favouring extraterritoriality of jurisdiction is manifested in numerous cases and by a wide array of authoritative documents. For example, in competition matters, the EC enjoys the authority to take any decision affecting institutions doing business within the EU but founded outside the EU. The EC exercised this power preventing a proposed merger between two US companies-General Electric and Honeywell.[75]

---

72 The GDPR, Article 83.

73 Penal Code, Malaysia, Act no. 574, Laws of Malaysia, as at 1 January 2015.

74 European Commission, "Rules of Procedure, 2010: Article 29 Data Protection Working Party," October, no. Lx: 1–8.

75 Comp, Case No, Rail Gourmet, and Gourmet Nova. 2002. "Regulation (EEC) No 4064 / 89" 9 (4064).

Similarly, Distance Selling Directive postulates that consumers cannot be deprived of protection approved by the Directive even by a preference of law clause under a contract wherever the chosen non-EU country's law gives the minimum advantage in comparison with EU law.[76] Again, in a Directive on Commercial Agents, the European Court of Justice held that where a business agent, appointed by an outside principal works within EU Community, the principal cannot evade provisions of the Directive by use of a contractual clause specifying that law of a third nation applies to that business activities.[77]

The similar stand of the EU is manifested in the Code of Conduct for Computer Reservation Systems (CRS's) as used in the aviation industry.[78] Accordingly, if a system is accessed from an EU member state, no matter whether the main appliance of the system is established in the EU or not, and processing of data is carried on by this system through any terminal in EU or not, EU law would automatically apply. For example, Article 3 (1) of the GDPR states,

> 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.

To conclude, while applying the extraterritorial jurisdiction over non-EU establishments, the EU examines whether such

---

76 "Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in Respect of Distance Contracts." 2014. In *Fundamental Texts on European Private Law*. Hart Publishing. doi:10.5040/9781472559500.0010.

77 "Directive 86/653/EEC of 18 December 1986 on the Coordination of the Laws of the Member States Relating to Self-Employed Commercial Agents." 2014. In *Fundamental Texts on European Private Law*. Hart Publishing. doi:10.5040/9781472559500.0013.

78 "Regulation (EC) No 80/2009 of the European Parliament and of the Council of 14 January 2009 on a Code of Conduct for Computerised Reservation Systems and Repealing Council Regulation (EEC) No 2299/89," Article, 11, accessed April 15, 2020, https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32009R0080&from=EN.

aspiration meets certain requirements, especially, the 'community dimension', 'concentration' etc.[79]

2. Statute of the International Court of Justice

The Statute of the International Court of Justice explicitly acknowledges the extraterritorial jurisdiction of States. Article 38 of the ICJ Statute, for example, asserts, the ICJ can decide a case between contesting parties following rules of international conventions explicitly consented by disputing countries; international custom, as proof of generally accepted law, and common principles of law approved by civilized nations.

From the provisions of Article 38 of the ICJ Statute, we can further assume that there are some other mechanisms, such as international instruments, international custom, and general principles of laws of the civilized nations by which legality of extraterritorial jurisdiction of States can be examined. For the sake of clarification, all these mechanisms are elaborated in the following.

3. International instruments

Contemporary international instruments hold some sort of persuasive influence and obligatory legal force to protect civil and human rights relating to privacy. Subject to reservations, these instruments impose certain mandatory compliance issues over corporations, governments and all other endorsers.[80] The list of those international instruments includes, *inter alia*:

a) Universal Declaration of Human Rights, 1948;[81]
b) International Covenant on Civil and Political Rights, 1966;[82]

---

79 European Commission, "Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the InternetInternet by Non-EU Based Web Sites," 5035/01/EN/Final WP 56 (May 30, 2002): 4.

80 Ray William London, "Comparative Data Protection and Security Law: A Critical Evaluation of Legal Standards" (PhD Diss., University of South Africa, 2013), 138.

81 Article 12.

82 Article 17.

c) Convention on the Rights of the Child, 1989;[83]
d) International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990;[84]
e) UN General Assembly Guidelines Concerning Computerized Personal Data Files, 1990.[85]

During the 1970s, the world community began to realize the necessity of introducing a global privacy policy standard as trans-border data flows were increasingly becoming a fact.[86] Even some policymakers apprehended that data security offered in national regimes were likely to be bypassed in the cross-border data processing activities. Michael D.Kirby, for example, remarks that certain principles, rules or guidelines were to be farmed and agreed upon at the international arena.[87] Eventually, two international instruments, i.e. the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines), 1980 and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) of the Council of Europe, 1981 had attempted to formulate the guiding principles encompassing privacy for generating harmonized data protection standards.[88]

It is noteworthy that both these documents recognize the issue of extraterritoriality of data protection regulations. For example, to describe 'Basic Principles of International Application', paragraphs 15-18 of OECD Guidelines refer to the term 'extraterritoriality', whereas paragraph four of the preamble of Convention 108 states, "reaffirming at the same time their commitment to freedom of

83 Article 16.
84 Article 14 and 15.
85 Article 9.
86 Adriana CM Nugter, *Transborder Flow of Personal Data within the EC a Comparative Analysis of Princiepstat.* Kluwer Law Intl, 1990: 20; Brendan Van Alsenoy, "Regulating Data Protection: The Allocation of Responsibility and Risk among Actors Involved in Personal Data Processing" (PhD Diss., Katholieke Universiteit Leuven, 2016), 155.
87 Michael D Kirby, "Transborder Data Flows and the Basic Rules of Data Privacy," *Stanford Journal of International Law* 16 (1980): 27.
88 Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Cornell University Press, 1992: 136.

information regardless of frontiers". Thus, the incorporation of extraterritoriality of jurisdiction is not a new thing rather it is a universally accepted norm of international law that is usually practised by diverse international instruments from long ago.

4. Customary international law

States apply territorial claims based on certain other principles of international law, such as territoriality principle, protective principle, passive personality principle etc.[89] Whereas, in respect of online conduct, States increasingly exercise their jurisdictions extraterritorially employing especially, effects doctrine, objective territoriality principles etc.[90] To understand each of these principles, a brief discussion is offered below.

(a)The territorial principle

Under the territorial principle, jurisdiction is determined based on activities carried on within the territorial boundary of States only.[91] The territorial principle means that States have complete jurisdiction over persons, assets and things within their boundary encompassing both subjective and objective territoriality.[92] Thus, according to this principle, States cannot extend their territorial scope outside their boundaries, unless it is coupled with the effects doctrine.

(b) The effects doctrine

The effects doctrine refers to the principles where an activity carried on outside the territorial jurisdiction of any State has effects on that

89 "Restatement (Third) of Foreign Relations Law of the United States," American Law Institute (1987): § 402 and § 403.

90 Wimmer, "The Long Arm," 17.

91 Cedric Ryngaert, *Jurisdiction in International Law,* (Oxford University Press, USA, 2008), 42.

92 Amanda Zambellas, "Exploring the Boundaries of International Law" (2016), accessed September 29, 2019, http://doer.col.org/handle/123456789/6253.

State.[93] The idea is nearly correlated to the objective territoriality principle but does not require things, equipment or establishments to be placed within State territory.[94] Although there are widespread criticisms against this doctrine from many legal scholars, it is extensively employed in regulating the behaviour of individuals using the internet.[95] Professor Kuner, for example, remarks that it is an 'open-ended' notion in a globalised economy, where everything affects each other.[96] Some scholars argue that the GDPR adopts the effect doctrine for applying extraterritorial jurisdiction through its Article 3 (2) given stresses on the place of probable harmful effects but discarding processing place of the operator.[97]

(c) The objective territoriality principle

Another relevant principle is the objective territoriality principle, which means a notion, where an act in question was started abroad but some components or the final parts are accomplished within the State's territory.[98] Some authors argue that along with the geographical jurisdiction, it is equally essential to restrict virtual jurisdiction, in which conventional territoriality principle is an obsolete idea, and this, eventually, paves the way of applying extraterritoriality of jurisdiction through objective territoriality principle.[99] Arguably, by Article 3 (2), the GDPR employs extraterritorial jurisdictional claims based on the objective territoriality principle, as it aims to regulate the things or behaviour

---

93 Edwin D Dickinson, "Introductory Comment to the Draft Convention on Jurisdiction with Respect to Crime," *American Journal of International Law* 29, no. 439: 455.

94 International Law Commission, Report. "On the Work of its Fifty-Eighth Session, UN Doc." *A/CN* 4 (2006).

95 Ibid.

96 Kuner, "Data Protection Law (Part 1)," 190.

97 Azzi, "The Challenges Faced," 131.

98 Ryngaert, *Jurisdiction in International Law*, 76. See also, Kuner, "Data protection law (Part 1)," 188.

99 Julia Hörnle, "Juggling more than Three Balls at once: Multilevel Jurisdictional Challenges in EU Data Protection Regulation," *International Journal of Law and Information Technology* 27, no. 2 (2019): 165.

(of overseas institutions which offer goods or services or monitor behaviour of EU residents) within the boundary of EU.

(d) The passive personality and the protective principle

Sometimes, territorial jurisdiction lies on the passive personality principle that ascertains jurisdiction depending on the citizenship of the sufferer.[100] Apart from exercising jurisdictional power over citizens for their actions done overseas, at times, States can exercise their jurisdictional authority against foreigners as well as for committing activities against their citizens. Ordinarily, this power is exercised in a limited manner in the context of some serious crimes only, for example, terrorist attacks or killings, and applies occasionally in some civil litigation too in some jurisdictions.[101]

For example, even though conventionally the US did not support exercising territorial authority based on this principle, but recently its courts have approved the principle in some specific cases, for example, in the instances of terrorism.[102] The protective principle, on the other hand, widens the notion to enable States to defend themselves rather than its inhabitants from destructive activities caused outside of their boundary.[103]

(e) The principles of comity

The notion of reasonableness as specified in the 3rd Restatement has a closer connection with the concept of comity that usually appears as a 'golden rule' among States. The principle of comity provides that every nation should value the interests, policies and laws of other nations which are similar to their own.[104] In particular, in respect of

---

100 Ryngaert, *Jurisdiction in International Law*, 88, 96. See also, Kuner, "Data protection law (Part 1)," 188.

101 "Restatement (Third)," § 402 cmt. g. See also, Kuner, "Data Protection Law (Part 1)," 188-189.

102 *US v. Bin Laden*, 92 F. Supp. 2d 189 (S.D.N.Y. 2000).

103 Ryngaert, *Jurisdiction in International Law*, 96. See also, Mann, Frederick Alexander. *The Doctrine of Jurisdiction in International Law*. Martinus Nijhoff, 1964: 80.

104 Joel R Paul, "Comity in International Law," *Harvard International Law Journal* 32 (1991): 1. See also, *Hilton v. Guyot*, 159 U.S. 113, 16 S. Ct. 139, 40 L. Ed. 95 (1895).

court proceedings, comity refers to a rule or principle by which an individual or proprietary rights emanated from laws or legal proceedings of a foreign country are acknowledged and implemented in national courts provided that it cannot be incompatible with any law or government policy of State which invokes that principle.[105]

There remain questions on how jurisdiction can be ascertained for a person or activity which stands between concurrent jurisdictions of two States. In such a condition, the person or that act will lie under such jurisdiction which possesses greater interests.[106] How can the concurrent jurisdictional issue be settled, where the use of the internet is in question. Professor Kuner remarks, to determine the exact jurisdiction in cases, where the internet or cyberspace are used, the courts should take into account certain things, for example, the application of cookies or other related technologies by other States; the location of the data controller and data subject, and the place where the unlawful activities happened, and where the personal data is processed and stored.[107]

Thus, it has become clear that the EU can exercise its extraterritorial jurisdictional claims over institutions beyond boundaries based on the above principles. Cedric Ryngaert summarizes, the EU can extend its extraterritorial jurisdiction over institutions outside the EU at least based on the combination of three principles, for example, the effects doctrine, the passive personality principle, and the objective territoriality principle.[108]

5. The laws of civilized nations

This is another important basis of customary international law which can evaluate municipal laws of a State or region and their corresponding jurisdictional reach. Despite assessing all, the evaluation of some selective jurisdictions would be pretty enough for evaluating authority and legitimacy of extraterritorial jurisdiction of

---

105 Herbert Barry, "Comity," *Virginia Law Review* (1926): 353-375; *Hartford Fire Ins. Co. v. California*, 509 U.S. 764, 113 S. Ct. 2891, 125 L. Ed. 2d 612 (1993).

106 "Restatement (Third)," § 402 cmt. E.

107 Kuner, "Data Protection (Part 2)," 227-247.

108 Cedric Ryngaert, "Symposium Issue on Extraterritoriality and EU Data Protection," *International Data Privacy Law* 5, no. 4 (2008): 221.

the GDPR. In recent times, extraterritorial applications of jurisdiction have become widespread, especially in data privacy, cybersecurity, or ICT laws. This is even exercised by nations outside the EU, EEA, or countries without an adequacy decision.

Section 9 (1) of the Computer Crimes Act, 1997 of Malaysia, for example, affirms that if any person commits any crime under this law being outside Malaysia, this enactment would apply against him, irrespective of nationality and citizenship, and in the manner that as if he commits the crime within Malaysia.[109] Similarly, Section 1302 (2) (ii) (II) and (iii) of the Children's Online Privacy Protection Act (COPPA) of the USA applies to foreign establishments which deliberately process personal data of US children or target them through their websites.[110] Likewise, section 11 of the Computer Misuse and Cybersecurity Act, 2017 of Singapore provides that provisions of law shall apply to any individual irrespective of his citizenship or nationality within and outside Singapore.[111]Similarly, section 5A and 5B of the Australian Privacy Act, 1988 provides that this law applies to all territories outside Australia, and especially, to any organisation or small business operator, that has an 'Australian link'.[112] Article 75 of Protection of Personal Information, 2017 of Japan asserts that the Act shall apply to any entity which is established outside Japan but processes personal data of residents of Japan.[113] In the same way, Article 51 (2) of the Personal Information Protection Act, 2012 of Taiwan affirms that provisions of this Act apply to any public and private body, who processes, collects or uses personal data of residents of China from outside the Chinese Republic.

It is pertinent to note that in respect of extraterritorial scope, the Malaysian PDPA provides that the Act applies to a person not established in Malaysia, but uses equipment in Malaysia for

---

109 Computer Crimes Act 1997, Malaysia, Act no. 563, Laws of Malaysia, Incorporating all amendments up to January 1, 2006.

110 Children's Online Privacy Protection Act (COPPA), USA, 15 U.S.C. §§ 6501-6506, came into effect on September 30, 2019.

111 Computer Misuse and Cybersecurity (Amendment) Bill, Singapore, Act no. 22 (2017).

112 Privacy Act 1988, Australia, Act no. 119: 294.

113 Personal Information Protection Commission, 2016, Japan (Amended Act on the Protection of Personal Information) (Tentative Translation)..

processing personal data except transit through Malaysia.[114] Furthermore, the PDPA postulates that it shall not apply to any 'personal data processed outside Malaysia' unless that data is processed further in Malaysia.[115] Therefore, the Malaysian PDPA also acknowledges the extraterritorial jurisdictional claims though differently from the GDPR. All these constructions eventually support the wider territorial scope of the GDPR.

6. The reasonableness test

The above constructions, nevertheless, are not absolute, rather they can be challenged in many jurisdictions on different grounds. Kurt Wimmer, for example, observes that the US authority can deny the extraterritorial application of the GDPR arguing that such jurisdiction is unreasonable under the 3rd Restatement test and extraterritoriality provision conflicts with the principles of comity. Even the US can challenge the application of extraterritorial application of the GDPR based on rights granted for the freedom of speech and press by the First Amendment of its Constitution contending that the freedom of expressions of the publishers can outweigh EU's aspirations of protecting the right to privacy of its individuals.[116]

Thus, from the US context, mere satisfaction of any of the stated principles is not sufficient to justify the application of territorial jurisdiction unless they satisfy the reasonableness test.[117] Under section 403 of the Restatement (Third), reasonableness is tested case by case subject to fulfilment of a lot of factors, including;

> …links of territory, links of nationality, justified expectations, the interests of the regulating state, the interests of other states, the interests of the international system, and the likelihood of conflict.[118]

---

114 PDPA, Malaysia, Section 2 (2) (b).

115 PDPA, Malaysia, Section 3 (2).

116 Wimmer, "The Long Arm," 18.

117 "Restatement (Third)," § 403(1).

118 Ibid, § 403(2). See also, William S. Dodge, "Jurisdictional Reasonableness under Customary International Law: The Approach of the Restatement (Fourth) of Us Foreign Relations Law," *QIL-Questions of International Law* 62 (October 2019): 8.

If any of these conditions are not meet, the court may determine that there is no jurisdiction at all.[119] Therefore, it has become clear that the extraterritorial scope of the GDPR is justified under international law, and especially, subject to fulfilment of the reasonableness test. Despite the above analysis, it is also important to clarify how the EU can implement the extraterritorial jurisdiction under the framework of the GDPR. Further explanation on this is provided in the next part of this article.

ENFORCEMENT OF EXTRATERRITORIAL SCOPE OF THE GDPR

The extraterritoriality of jurisdiction witnesses tremendous challenges, especially in the context of a non-physical existence of cyberspace. Besides, extensive territorial jurisdiction confronts with several other procedural impediments also, ranging from investigation to sanction stage.[120] Goldsmith and Wu note that "as a general matter, nations can exercise coercive powers within their borders but not beyond".[121] Despite numerous barriers, the GDPR aims to apply its extraterritorial jurisdiction all over the globe since its inception. In implementing the jurisdiction with extraterritorial reach, the GDPR resorts to several mechanisms, such as the cooperation mechanism, consistency mechanism, and several indirect mechanisms, including reputational impact. These are evaluated below.

1. The cooperation mechanism

Without having cooperation among States, especially, on investigation measures and recognition of foreign judgements, the attainment of extraterritorial application of jurisdiction is almost impossible. The cooperation mechanism includes, *inter alia*, exchange of information, mutual collaboration, combined operations etc.[122] As per the norms of international law, a State must obtain the

---

119 Ibid, § 403 (2) (a) - (h).

120 Azzi, "The Challenges Faced," 128.

121 Wu and Goldsmith, *Who Controls the Internet?,* 156.

122 Julia Hörnle, "Juggling More than Three Balls at Once: Multilevel Jurisdictional Challenges in EU Data Protection

consent of its foreign counterpart and the consent of parties for carrying on activity within a foreign territory which falls under the absolute authority of foreign public officials, e.g., the investigating authorities.[123]

To obtain such consent, States can rely on mutual agreements, which is widely exercised, especially in respect of transnational criminal offences, and data protection. For example, in 1996, the Data Protection Authority (DPA) of German received the consent of the Citibank, a US financial organization, while conducting an audit on data processing activities of German credit cardholders.[124] Likewise, the DPA of Spain carried on another inspection on data processing facilities of a data recipient in Colombia by relying on an agreement which approved that investigation.[125]

The GDPR urges for strong coordination among all supervisory authorities of EEA nations (the EU Member States, in addition to Iceland, Liechtenstein and Norway) to imply and support cross-border issue through the utilisation of some other mechanisms, like mutual cooperation, combined operation, and the one-stop-shop collaboration tool that offers an obligatory effort of maintaining a leading supervisory authority for the trans-border issues. The EU manages to handle cross-border issues grounded on public complaints by domestic supervisory bodies.[126]

2. The consistency mechanism

Consistency appears as a core to the rule of law and legal certainty, which is usually interconnected with teleology. It verifies the shortcomings of legal norms, fundamental rights and others are based

Regulation," *International Journal of Law and Information Technology* 27, no. 2 (2019): 152.

123 Kuner, "Data Protection (Part 2)," 232.

124 Ibid.

125 Ibid.

126 "First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities," European Data Protection Board, (EDPB) (2019): 2, accessed April 15, 2020. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf.

on the doctrine of proportionality.[127] Consistency is one of the key activities of the European Data Protection Board (EDPB) for applying the GDPR with extraterritoriality. The aim is to render policy guidance for different stakeholders and general people by interpreting the GDPR to facilitate a common view and apply provisions by the supervisory authorities.[128] It is worth noting that to date, the EDPB has approved 16 guidelines made by Article 29 Working Party (the EDPB's predecessor) and welcomed 5 other guidelines.[129] Howbeit, the consistency mechanism works based on two other tools, e.g., consistency opinion and dispute resolution.[130]

For several policy decisions, such as cross-border codes of conduct, adoption of contractual clauses, adoption of nationwide lists specifying the sort of processing, which is contingent upon a data protection impact assessment, national supervisory authorities must seek views of EDPB before taking its decision. The supervisory authority of any Member State, the Chairperson of EDPB or Commission may require EDPB for issuing a consistency opinion on any topic of general interest or issues that affect more than one EU nationals.[131] So far, the EDPB gave 28 opinions on national registers of processing based on a data protection impact assessment and 1 opinion on the rough executive arrangement for transfer of personal data among economic supervisory authorities within EEA and beyond.[132] At present, the EDPB keeps on giving its opinion on three ongoing procedures, including draft contract standard between processors and controllers, binding corporate rules, and interaction between e-Privacy Directive and the GDPR.[133]

---

127 Claes Granmar, "Global Applicability of the GDPR in Context," (August (2019): 12, accessed April 15, 2020, https://su.diva-portal.org/smash/get/diva2:1274839/FULLTEXT01.pdf.

128 EDPB, "First Overview," 6.

129 Ibid, 2.

130 Ibid.

131 Ibid.

132 Ibid, 6.

133 Ibid.

3. Reputational impact

Through its extraterritorial application, the GDPR has extended its long arm to cover the activities of many overseas companies since its commencement. Meanwhile, the French DPA (CNIL) inflicted the highest GDPR sanctions of €50 million against Google due to its failure to demonstrate precise users' guidelines for data sharing by many of its services.[134]In July 2018, UK's Information Commissioner's Office (ICO) imposed a fine of £500,000 against Facebook because of Cambridge Analytica scandal.[135] Besides, ICO also fined Equifax Ltd, a US-based credit risk assessment agency, for an amount of £500,000 for its failure of protecting the personal data of around 15 million UK residents during a cyberattack in 2017.[136]

In November 2018, the Dutch DPA [*Autoriteit Persoonsgegevens* (*AP*)] and ICO combinedly fined Uber a total of $1.17 million for a data breach incident that took place in 2016. In that fine, ICO's amount was £385,000 ($491,284), and Dutch's imposition was up to €600,000 ($679,257).[137] Consequently, due to the fear of reputational damage, many giant companies, such as IBM, Microsoft, Facebook, Google, Amazon etc. have taken initiatives and

---

134 "The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against Google LLC," CNIL, (Commission nationale de l'informatique et des libertés) last modified, January 21, 2019, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

135 "ICO Issues Maximum £500,000 Fine to Facebook for Failing to Protect Users' Personal Information," ICO, (Information Commissioner's Office), UK, last modified, October 25, 2018, https://ico.org.uk/facebook-fine-20181025?utm_source=twitter&utm_medium=iconews&utm_term=7e7dd63a-2bfd-407c-b985-c21fa7b16b6c&utm_content=&utm_campaign=%C2%A0.

136 "Equifax Ltd," ICO, (Information Commissioner's Office), UK, last modified, September 20, 2018, https://ico.org.uk/action-weve-taken/enforcement/equifax-ltd/.

137 Elizabeth Schulze, Uber Fined Nearly $1.2 Million by British and Dutch Authorities for 2016 Data Breach, CNBC, accessed April 15, 2020, https://www.cnbc.com/2018/11/27/uber-fined-more-than-1-million-dollars-by-uk-and-dutch-authorities.html.

are now GDPR compliant.[138] Thus, these giant corporations enable the GDPR to extend its extraterritorial scope to overseas institutions indirectly.

Arguably, if any entity outside the EU, for example, from Malaysia, processes personal data of EU residents by offering goods or service, or monitor the behaviour of EU residents, or in a condition where laws of EU Member States apply by dint of public international law, the GDPR shall apply to it. In case of any non-compliance, that Malaysian entity shall have to endure the same fate as undergone by Facebook, Google, Uber, Equifax etc.

CONCLUSION

The contemporary legal challenges encompassing data privacy are increasingly extraterritorial in nature because of numerous reasons, including the growing advancement of technology and increasing dependence thereof, today's data-based economy and modern business model. In this context, it is always advisable to make legal rules with global implications, otherwise, that would not serve the desired purposes. Paying heed to this, the EU extended its territorial reach by incorporating the provisions of extraterritoriality in Article 3 (2) of the GDPR.

However, extraterritorial jurisdiction is not an issue beyond dispute. Because of several dilemmas, for example, while a State attempts to enforce it, the other to oppose by dint of sovereignty principle, and this eventually, pushes two countries into a confrontation.[139] Furthermore, extraterritoriality of jurisdiction is evermore a debatable issue under international law, not because it

[138] Matt Burgess, "How Apple, Facebook and Google Are Changing to Comply with GDPR," Wired, last modified, May 24, 2018, https://www.wired.co.uk/article/gdpr-facebook-google-analytics-apple-amazon-twitter.

[139] Alan V Lowe, "The Problems of Extraterritorial Jurisdiction: Economic Sovereignty and the Search for a Solution," *International & Comparative Law Quarterly* 34, no. 4 (1985): 724.

supports attack on territorial integrity and legal imperialism, but because of the lack of certainty and clarity, it entails.[140]

Given that, there is no ambiguity in the provisions of extraterritorial jurisdiction of the GDPR. For example, the GDPR aspires, by Article 3, to extend its territorial reach outside the EU on fulfilment of two specific conditions, i.e., the establishment in the EU or targeting the EU. The GDPR clearly explains what is meant by the establishment in the context of the EU, and what is targeting. Accordingly, both data controllers and processors are aware of these, and they also know who they target through their activities. Additionally, the provisions of extraterritoriality have been further stated and clarified in recital 24. Furthermore, EU authorities wish to offer essential certainty, if required after observing the evaluation report of EC to be submitted on 25 May 2020 under Article 97 of the GDPR.[141]

It is, therefore evident that without confronting with State's sovereignty principle, extraterritorial jurisdiction is justified by a wide array of principles of customary international law, particularly by effects doctrine, passive personality principle and objective territoriality principle.[142] Additionally, extraterritoriality of jurisdiction is recognized by principles of laws of the civilized nations as discussed earlier under sub-heading 'laws of the civilized nations' at Part VI, subject to fulfilment of reasonableness test.

Conversely, if States consider the extraterritoriality approach of the EU is unjust, unfair, or unreasonable, they may have to pass 'blocking' enactment,[143] which may ultimately, create distrust and non-cooperation among nations. Hugo Grotius once asserted that

---

140 Humberto Cantú Rivera, "Developments in Extraterritoriality and Soft Law: Towards New Measures to Hold Corporations Accountable for their Human Rights Performance?" *Anuario mexicano de derecho internacional* 14 (2014): 732.

141 Paul De Hert and Michal Czerniawski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context," *International Data Privacy Law* 6, no. 3 (2016): 243.

142 Ryngaert, "Symposium," 221.

143 Svantesson, "The Extraterritoriality of EU," 94.

'wherever judicial resolution does not work, the battle starts'.[144] Above all, customary international law is leaning towards upholding than prohibiting the territorial expansion of the EU. Thus, Christopher Kuner urges for greater harmonisation of laws, coordination among the regulatory bodies, technical alternatives, promotion of the theory of comity or reasonableness, and closer interaction among privacy and jurisdiction experts.[145] Finally, it can be concluded that extraterritorial jurisdiction of the GDPR does not hamper the territorial integrity of States, or regions, rather it ensures better protection of privacy and personal data for a large number of people in Europe and beyond. Thus, optimists may hope that the GDPR would appear as a global data privacy gold standard by breaking borders. Meanwhile, the GDPR has achieved that golden benchmark in the sphere of data protection law and scholarship.

144 Grotius, Hugo. *Hugo Grotius on the law of war and peace*. Cambridge University Press, 2012: 81. See also, Svantesson, "The Extraterritoriality of EU," 101.

145 Kuner, "Data Protection (Part 2)," 242-246. See also, Svantesson, "The Extraterritoriality of EU," 96.