The European Journal of International Law Vol. 32 no. 4

Conflicts and Tentative Solutions to Protecting Personal Data in Investment Arbitration

Jie (Jeanne) Huang*

Abstract

Personal data protection in investment arbitration is increasingly important as more and more countries enact mandatory personal data protection laws and the COVID-19 pandemic makes online hearings the new normal. Tribunals have to consider critical, yet unresolved, normative questions, such as (i) how data protection laws would influence the trend towards transparency in investment arbitrations brought pursuant to modern investment treaties; (ii) whether a party can invoke a data protection law to reject access to fundamental documents and completely shift the power in an arbitration proceeding; (iii) whether it is good to have multiple data protection laws directly applicable in an investment arbitration; and (iv) whether the so-called Brussels Effect may take hold of investment arbitration. These questions directly address the alleged legitimacy crisis of investment arbitration (for example, procedural transparency and efficiency) in the digital era. They also have a critical impact on the fairness of proceedings and are closely related to the protection of fundamental human rights and the concern of digital surveillance. This article comprehensively maps the consensual and mandatory applications of data protection laws in investment arbitration. Adopting comparative-law and conflict-of-laws methodologies, it intends to provide tentative solutions to the four questions mentioned above.

1 Introduction

Personal data protection in investment arbitration is increasingly important as more and more countries enact local data protection laws[1] and the COVID-19 pandemic

* Jie (Jeanne) Huang, Associate Professor, University of Sydney Law School, Australia. Email: Jeanne.huang@sydney.edu.au. The research for this article was partially funded by the China Social Science Fund (16BFX202). The author is very grateful for the three anonymous referees' comments. All errors are mine.

[1] E.g. Council Regulation (EU) 2016/679 (GDPR), OJ 2016 L 119/1; California Consumer Privacy Act, 23 September 2018, effective on 1 January 2020, www.isipp.com/resources/

makes online hearings the new normal.[2] The challenges to personal data protection in investment arbitration are not entirely the same as those in commercial arbitration because the Mauritius Convention on Transparency (Mauritius Convention)[3] and the UNCITRAL Rules on Transparency in Treaty-based Investor-State Arbitration (Rules on Transparency)[4] require investment arbitration proceedings to be transparent, while commercial arbitration is usually confidential.[5] Investment arbitration inheres in the tension between the multinational approach to transparency adopted by the Mauritius Convention and the unilateral and sovereignty approach adopted by domestic data protection laws.[6] Moreover, data protection in investment arbitration also

---

full-text-of-the-california-consumer-privacy-act-of-2018-ccpa/, last visited 9 June 2021. China incorporated the protection of personal data into the Chinese Civil Code (Minfa Dian), Order no. 45, 28 May 2020, effective 1 January 2021 Arts 1032–1037. The 'local data protection law' discussed in this article is limited to personal data protection laws of a state or a regional economic and political union such as the European Union (EU). It does not include data protection international treaties such as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data concluded in Strasbourg on 28 January 1981, entry into force on 1 October 1985, ETS No. 108, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108; the Organisation for Economic Co-operation and Development's Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data (OECD 2013 Recommendation), 11 July 2013, available at https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, or the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules and the Privacy Framework (APEC Privacy Framework), August 2017, APEC#217-CT-01.9, available at https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf.

2 E.g. Joint Statement on Arbitration and COVID-19, 16 April 2020, available at https://sccinstitute.com/media/1658123/covid-19-joint-statement.pdf, which was issued by 13 arbitration institutions; 'Virtual Hearings: The New Normal', *Global Arbitration Review*, 27 March 2020 available at https://globalarbitrationreview.com/virtual-hearings-the-new-normal. In this article, personal data and personal information are used interchangeably and refer to information relating to an identified or identifiable natural person. See GDPR, *supra* note 1, Art. 4(1). International Council for Commercial Arbitration (ICCA), New York City Bar and International Institute for Conflict Prevention and Resolution, Protocol on Cybersecurity in International Arbitration (Protocol on Cybersecurity), ICCA Reports no. 6 (2020), at 8; ICCA and International Bar Association (IBA), The ICCA-IBA Roadmap to Data Protection in International Arbitration, ICCA Reports no. 7 (2020), Explanatory Note 5: What 'Personal Data' Is Processed during an Arbitration; ICCA and IBA, The ICCA-IBA Roadmap to Data Protection in International Arbitration, ICCA Reports no. 7 (2020), at 14–32 (indicating that the publication of parties with submissions and arbitral awards (redacted or otherwise), including the collection of evidence or maintenance of a proceeding's confidentiality, may also involve personal data). See also International Chamber of Commerce (ICC), Information Technology in International Arbitration, ICC Commission Report (2017), at 2.

3 United Nations Convention on Transparency in Treaty-based Investor-State Arbitration (Mauritius Convention) 2014.

4 UNCITRAL Rules on Transparency in Treaty-based Investor-State Arbitration (Rules on Transparency), GA Res. 68/109, 1 April 2014, https://uncitral.un.org/en/texts/arbitration/contractualtexts/transparency; Mauritius Convention, *ibid.*, Art. 2, provides the application of the Rules on Transparency.

5 N. Blackaby *et al.*, *Redfern and Hunter on International Arbitration* (6th edn, 2015), at 30 (indicating that being private and confidential is one of the key features of international commercial arbitration). Caron and Shirlow, 'The Multiple Forms of Transparency in International Investment Arbitration: Their Implications, and Their Limits', in T. Shultz and F. Ortino (eds), *Oxford Public International Law* (2020) 469, at 490 (describing three types of transparency: transparency as availability; transparency as accessibility; and transparency as participation and commenting on the Rules on Transparency, *supra* note 4).

6 Huang, 'Applicable Law to Transnational Personal Data: Trends and Dynamics', 21 *German Law Journal* (2020) 1283, at 1296–1301 (analysing the spread-out unilateral applicable law approach).

differs from that of litigation at a national court because investment arbitration is confronted with messy conflict-of-data protection law issues,[7] while a national court often applies *lex fori* to decide how to protect personal data.[8]

Further, participants in state-to-state dispute resolution at international tribunals (for example, the International Court of Justice [ICJ]) can enjoy privileges and immunities from domestic laws.[9] However, not all participants in investment arbitration can rely on privileges and immunities under public international law to be exempt from complying with domestic data protection laws.[10] In these contexts, responding to the booming local mandatory laws for data protection, this article focuses on four normative questions in investment arbitration: (i) how local data protection laws would influence the trend towards transparency in investment arbitrations brought pursuant to modern investment treaties; (ii) whether a party in an investment arbitration can use a local data protection law to reject access to fundamental documents and completely shift the power in arbitral proceedings; (iii) whether it is good to have multiple data protection laws directly applicable in an investment arbitration; and (iv) whether the so-called Brussels Effect[11] may take hold on investment arbitration.

These questions influence the development of investment arbitration in the digital era because they directly address the alleged legitimacy crisis of investment arbitration caused by its perceived lack of, for example, procedural transparency and efficiency.[12] The questions also have a critical impact on the fairness of proceedings if a party can rely on a local data protection law to block the other party's access to fundamental information or reject the other party's legitimate request for data protection. They are also closely related to the protection of fundamental human rights and the concern of

[7] See Bismuth, 'Anatomy of the Law and Practice of Interim Protective Measures in International Investment Arbitration', 26 *Journal of International Arbitration* (2009) 773, at 773–821 (arguing that investment arbitration tribunals have interpreted the *lex arbitralis* in light of international tribunals and that the *imperium* of an investment arbitrator is different from that of a domestic court).

[8] E.g. in Australia, how to protect personal data is a procedure issue because it is about the mode or conduct of court proceedings and *lex fori* should be applied. *John Pfeiffer Pty Ltd v. Rogerson*, (2000) 203 CLR 503, para. 99.

[9] E.g. Charter of the United Nations, 1945, 1 UNTS 15, Art. 105 provides that '[r]epresentatives of the Members of the United Nations and officials of the Organization shall similarly enjoy such privileges and immunities as are necessary for the independent exercise of their functions in connection with the Organization'. See also Convention on the Privileges and Immunities of the United Nations, art IV, ss 11 (a), 12, 18, and 22. Convention on the Privileges and Immunities of the United Nations 1946, 1 UNTS 15, Art. V, ss 13, 14, 19, Annex 6. For transparency in other state-to-state tribunals, see Neumann and Simma, 'Transparency in International Adjudication', in A. Bianchi and A. Peters (eds), *Transparency in International Law* (2013) 436, at 436–476.

[10] J. Huang and D. Xie, 'Data Protection Law in Investment Arbitration: Applicable or Not?', 37 *Arbitration International* (2021) 167, at 167–196.

[11] For a detailed discussion of the Brussels Effect, see section 4.D.

[12] E.g. IBA Arbitration Subcommittee on Investment Treaty Arbitration, Consistency, Efficiency and Transparency in Investment Treaty Arbitration, November 2018, at 2 (indicating that 'increasing consistency, efficiency and especially transparency foster the legitimacy of investment-state dispute settlement').

digital surveillance.[13] In order to explore the four questions, this article comprehensively maps both the consensual and mandatory applications of local data protection laws in investment arbitration. The consensual application includes parties' choice of law, the *lex arbitri*, and treaties or arbitral rules to which an investment arbitration is pursuant. Local data protection laws can also be applied as mandatory laws; however, the mandatory application can be exempted through public international law privileges and immunities.[14]

This article focuses on addressing the four normative questions mentioned earlier: transparency versus privacy; the balance of power; the application of multiple data protection laws; and the Brussels Effect. The major research methodologies used in this article are comparative studies and conflict-of-laws analysis. For example, to analyse the applicability of local data protection laws, the article compares the investment chapters of the four most recent free trade agreements (FTA) and the investment treaties concluded by the major jurisdictions in the world – namely, the US-Mexico-Canada Agreement (USMCA),[15] the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP),[16] the China-Australia FTA[17] and the EU-Vietnam Investment Promotion Agreement (EVIPA).[18] The article also contrasts the General Agreement on Trade in Services (GATS)[19] with investment treaties and suggests that the former provides more guidance to tribunals who need to determine the applicability of a data protection law of a respondent state. The article further distinguishes

[13] Cole and Fabbrini, 'Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders', 14 *International Journal of Constitutional Law* (*IJCL*) (2016) 220, at 223 (arguing that 'protection of personal data is founded upon human rights treaties within the EU'); P.M. Schwartz and J.R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (1996), at 39 (arguing that the gathering of personal data in the USA is 'to weaken the individual capacity for critical reflection and to repress any social movements outside their control').

[14] There are many activities in an investment arbitration. Privileges and immunities under public international law only apply to activities that are 'strictly necessary' to an investment arbitration. See *European Molecular Biology Laboratory (EMBL) v. Federal Republic of Germany*, Award, 29 June 1990, reprinted in 105 ILR (1997) 1 (holding that an 'official activity' of the organization must be 'strictly necessary' to the exercise of the organization's functions); see also *Mukoro v. European Bank for Reconstruction and Development (EBRD)*, Employment Appeal Tribunal, United Kingdom (UK), 19 May 1994, reprinted in 107 ILR (1997) 604 (this case considered whether an international organization should enjoy jurisdictional immunity from a claim of racial discrimination in an employment dispute in the UK).

[15] US-Mexico-Canada Agreement (USMCA) 2020, available at https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

[16] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) 2018, available at https://www.dfat.gov.au/trade/agreements/Pages/trade-agreements. It was effective on 30 December 2018 for Australia, Canada, Japan, Mexico, New Zealand and Singapore, and on 14 January 2019 for Vietnam.

[17] The China-Australia Free Trade Agreement (the China-Australia FTA), 20 December 2015, available at https://www.dfat.gov.au/trade/agreements/in-force/chafta/official-documents/Pages/official-documents.

[18] The EU-Vietnam Investment Protection Agreement (EVIPA), 30 June 2019, available at https://investmentpolicy.unctad.org/international-investment-agreements/treaties/treaties-with-investment-provisions/3616/eu---viet-nam-investment-protection-agreement-2019-.

[19] General Agreement on Trade in Services (GATS), 1869 UNTS 183.

the confidentiality protection in traditional arbitration law from the privacy protection in the data protection regime.

Besides the introduction, this article has five sections. The second section analyses consensual application of a local data protection law according to the *lex arbitri*, the applicable treaties or procedural rules in investment arbitration. It argues that the *lex arbitri* may include a local data protection law applicable at the seat. Regarding the applicable treaties, it argues that the USMCA, the CPTPP and the China-Australia FTA provide more opportunities to apply the data protection law of the respondent state compared with the law of the investor's home state. This imbalance lays down the potential to shift the power in arbitral proceedings towards the respondent state. Regarding the arbitral rules, it analyses confidentiality orders to protect personal data and argues that personal data protection expands the scope of protecting confidential information in investment arbitration. The third section uses the General Data Protection Regulation (GDPR) as an example to scrutinize the application of a local data protection law as a mandatory law.[20] It analyses the possibility of and the limits to invoking privileges and immunities under public international law to exempt the mandatory application of the local data protection law. The fourth section addresses the four normative questions mentioned earlier. It argues that personal data protection would not prompt tribunals to reverse transparency requests and return to more secretive proceedings. It suggests that tribunals should draw insights from the two-tier analysis under Article XIV of the GATS to balance the power between arbitral participants in investment arbitration. It proposes a functional approach to addressing the messy conflicts arising from the application of multiple data protection laws in an investment arbitral proceeding. It analyses the possibility, and associated challenges, of the Brussels Effect taking hold in investment arbitration. The fifth section concludes the article.

2 Consensual Application

Arbitration is based on party autonomy. If parties have already chosen a data protection law, that law should be applied.[21] Besides the explicit choice of law, a local data protection law may be included in the *lex arbitri* due to parties' choice of the seat of arbitration. Consensual application of a local data protection law may also occur when the law is referred to in the treaties or procedural rules to which the arbitrations are pursuant. Consensual application should be the primary source for a tribunal in determining whether an investment arbitration is subject to a local data protection law.

A Lex arbitri

The *lex arbitri* is 'a body of rules which sets a standard external to the arbitration agreement, and the wishes of the parties, for the conduct of the arbitration'.[22] The

[20] GDPR, *supra* note 1.

[21] See Protocol on Cybersecurity, *supra* note 2, Principle 4.

[22] *Smith Ltd v. H International*, [1991] 2 Lloyd's Rep 127, at 130.

law of the seat of an arbitration is the *lex arbitri*.[23] Even if the parties have chosen a different procedural law for the arbitration, the law of the seat is still applicable. In *Union of India v. McDonnell Douglas*, the service contract was governed by Indian law and contained an arbitration clause that provided that arbitration was to be 'conducted' in accordance with the procedure provided by the Indian Arbitration Act 1940, whereas the 'seat' of the arbitration was to be London.[24] The English court held that, by the use of the word 'seat', the parties had chosen English law to govern the arbitration proceedings, and the reference to 'conducted' had the effect of contractually importing from the Indian Act provisions that were both concerned with the internal conduct of their arbitrations and not inconsistent with the choice of English arbitral procedural law.[25] Therefore, according to *Union of India*, the law of the seat – namely, English law – was to be applied to:

> (b) the external relationship between the arbitration and the courts, whose powers may be both supportive and supervisory, such as the grant of interim relief, procuring evidence from third parties and securing the attendance of witnesses, the removal of arbitrators and the setting aside of awards; and
> (c) the broader external relationship between arbitrations and the public policies of that place, which includes matters such as arbitrability and possibly also – more controversially – the impact on arbitration of social, religious and other fundamental values in each State.[26]

The law of the seat may include the data protection law applicable at the seat.[27] The underlying reason is that the law of the seat prescribes the relationship between an arbitration, on the one hand, and the courts and the public policies of the seat, on the other hand. Regarding the external relationship, the courts at the seat symbolize the regulatory authorities at the seat, which should include the government data regulation agency. Within the broader external relationship, the public policies of the seat cannot be excluded by an arbitration agreement.[28] Is the data protection law a public policy of the seat? If an investment arbitration is seated in the European Union (EU), the law of the seat should include the data protection law applicable at the seat. This is because

[23] Hill, 'Determining the Seat of an International Arbitration: Party Autonomy and the Interpretation of Arbitration Agreements', 63 *International and Comparative Law Quarterly* (2014) 517, at 519.

[24] *Union of India v. McDonnell Douglas Corp*, [1993] 2 Lloyd's Rep 48, at 48.

[25] *Ibid.* Vakharia, 'Splitting Procedural Law: Examining the Implications of Union of India v. Mcdonnell Douglas', 73 *Dispute Resolution Journal* (2018) 89, at 90.

[26] The Indian law applies to matters internal to an arbitration, such as the composition and appointment of a tribunal, requirements for an arbitral procedure and due process and the formal requirements for an award. See Henderson, 'Lex arbitri, Procedural Law and The Seat of Arbitration: Unravelling the Laws of the Arbitration Process', 26 *Singapore Academy of Law Journal* (2014) 886, at 887–888; see also Blackaby *et al.*, *supra* note 5, at 168–169.

[27] See Clifford and Scogings, 'Which Law Determines the Confidentiality of Commercial Arbitration?', 35 *Arbitration International* (2019) 391, at 398 (arguing that 'the obligation of confidentiality forms part of the procedural law in some jurisdictions' and the law of the seat should determine confidentiality).

[28] See UNCITRAL Model Law on International Commercial Arbitration 1985, 24 ILM 1302 (1985), Art. 34(2)(b)(ii).

the right to the protection of personal data is a fundamental human right and cannot be traded off, which is the EU's public policy.[29] The GDPR should be applied when its material and territorial scope are satisfied.[30] Therefore, it cannot be excluded by an arbitration agreement and should be applied to an investment arbitration seated in the EU.

The USA has no uniform data protection law like the GDPR.[31] A foreign business that collects, holds, transmits, processes or shares a US resident's personal data is subject to US federal data protection laws and may also be subject to the relevant state-based laws in the state where the data subject resides.[32] Therefore, whether a US data protection law represents public policy must be determined statute by statute. Different from the USA and the EU laws, the Chinese Civil Code distinguishes the protection of personal data from the right to privacy.[33] The protection of personal data is mixed with the Chinese government's plan to develop the local data industry.[34] As a result, Chinese personal data protection laws are closely linked with China's economic policy rather than social, religious and other fundamental values in China. However, the protection of personal data in China is also mingled with data sovereignty and national security, which can be considered to be Chinese public policy.[35] Therefore, if an investment arbitration is seated in China, the question whether a Chinese personal data protection law can be considered as the public policy of the seat should be determined case by case.

B *Treaties*

A local data protection law should be applied when a treaty to which an investment arbitration is pursuant says so. For example, in *Elliott Associates v. Korea*, the tribunal applied Korea's Personal Information Protection Act (PIPA) and accordingly held that relevant personal information should be redacted from submitted documents before publication.[36] The PIPA's application arose from the fact that the investment

[29] Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) 1950, 213 UNTS 222, Art. 8; Charter of Fundamental Rights of the European Union (EU Charter), OJ 2012 C 326/02, Article 8.1.

[30] GDPR, *supra* note 1, Arts 2, 3.

[31] Boyne, 'Data Protection in the United States', 66 *American Journal of Comparative Law* (2018) 299, at 299–343.

[32] S. Chabinsky and F.P. Pittman, 'The ICLG: Data Protection 2019—USA', available at https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa; see also *Watson v. Employer Liability Corp*, 348 US 66, at 72 (1954) (holding that a state 'may regulate to protect interests of its own people, even though other phases of the same transactions might justify regulator legislation in other states').

[33] Huang, *supra* note 6, at 1289–1292. Chinese Civil Code, *supra* note 1.

[34] Wu, 'Critique of Personal Data Information Privacy Protection under Big Data Technology' [Da Shuju Jishu Xia Geren Shuju Xinxi Siquan Baohu Lun Pinpan], 7 *Politics and Law* [*Zhengzhi yu Falv*] (2016) 116, at 129–131.

[35] See generally Cybersecurity Law of the People's Republic of China [Zhonghua Renmin Gongheguo Wangluo Anquan Fa], as adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China, 7 November 2016.

[36] PCA, *Elliott Associates, LP v. Republic of Korea*, 22 July 2019, PCA Case no. 2018–51, Procedural Order no. 4, paras 35, 43–45. (The tribunal concluded that, under the Personal Information Protection Act, protection from disclosure extends to information that is already in the public domain in circumstances where the information has been disclosed by the press.)

arbitration was brought pursuant to the US-Korea Free Trade Agreement (US-Korea FTA),[37] Article 11.28 of which defined 'protected information' as 'confidential business information or information that is privileged or otherwise protected from disclosure *under a Party's law*'.[38] '[A] Party's law' can be the law of the investor's home state or the host state.

The USMCA, the CPTPP, the China-Australia FTA and the EVIPA are the most recent investment treaties/FTAs concluded by the major jurisdictions in the world. The choice of a local data protection law can often be found in the treaty provisions dealing with, for example, the definition of protected information, special formalities and information requirements, transparency, the disclosure of information and the governing law. The definition of 'protected information' in the USMCA, the CPTPP and the China-Australia FTA is the same as the definition in the US-Korea FTA that is analysed in *Elliott*.[39] Although the EVIPA does not define 'protected information', it allows a party to designate information as confidential according to the law of the party.[40]

The USMCA, the CPTPP, the China-Australia FTA and the EVIPA similarly provide that, if a disputing party intends to use protected information in a hearing, it shall so advise the tribunal, and the tribunal shall make appropriate arrangements.[41] If parties have disputes regarding what information should be protected and how to protect it, which law should the tribunal invoke to resolve the dispute? The EVIPA appears to require the tribunal to consider the law of the investor's home state and the law of the respondent state equally.[42] In contrast, the USMCA, the CPTPP and the China-Australia FTA allow more opportunities for the application of the data protection law of the respondent state (that is, the investment host state). For example, Article 9.24 of the CPTPP indicates that '[n]othing in this Section … requires *a respondent* to make available to the public or otherwise disclose during or after the arbitral proceedings, … that it may withhold in accordance with Article 29.2 (Security Exceptions) or Article

[37] *Ibid.*, *Elliott* was administered by the Permanent Court of Arbitration (PCA) and the applicable procedural rules were the 2013 UNCITRAL Arbitration Rules. US-Korea Free Trade Agreement, 15 March 2012, available at https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text.

[38] *Ibid.*, Art. 11.28 (emphasis added). *Elliott*, *supra* note 36, Procedural Order no. 4, paras 14, 15. In Procedural Order no 1, 1 April 2019, para. 10.4, the tribunal defines 'protected information' as 'any information not in the public domain that is designated as such by a Party on grounds of commercial or technical confidentiality, special political or institutional sensitivity (including information that has been classified as secret by a government or a public international institution), or information in relation to which a Party owes an obligation of confidence to a third party'.

[39] E.g. CPTPP, *supra* note 16, Art. 9.1; China-Australia FTA, *supra* note 17, Art. 9.10 (g); USMCA, *supra* note 15, Art. 14.D.1.

[40] EVIPA, *supra* note 18, Art. 3.46.7; see also Rule 37 of Annex 7 of EVIPA (providing that '[e]ach Party and its advisers shall treat as confidential any information submitted to the arbitration panel and designated as confidential by the other party').

[41] USMCA, *supra* note 15, Art. 14.D.8.3; CPTPP, *supra* note 16, Art. 9.24.2; China-Australia FTA, *supra* note 17, Art. 9.17; EVIPA, *supra* note 18, Rule 37 of Annex 7.

[42] EVIPA, *supra* note 18, Art. 3.46.3. EVIPA integrates the Rules on Transparency, *supra* note 4. For details, see section 4.A.

29.7 (Disclosure of Information)'.[43] This means that an investment host state may apply its law to reject a data subject's right to access his or her data, such as requests to obtain confirmation that the data is being processed and to know the purpose of the processing and envisaged storage period.[44] Notably, Article 9.24 does not provide an equivalent ground for the investor to reject an investment host state's right to access personal data. This imbalance is further increased by Article 9.24.5, which allows 'a *respondent* to withhold from the public information required to be disclosed by its laws. The respondent should endeavour to apply those laws in a manner sensitive to protecting from disclosure information that has been designated as protected information'.[45] It is debatable what a 'sensitive' manner means.

Similarly, Article 9.17 (Transparency of Arbitral Proceedings) of the Investment Chapter of the China-Australia FTA also tips the scale in favour of the application of the data protection law of the respondent state. It explicitly provides that '*[w]ith the agreement of the respondent*, the tribunal shall conduct hearings open to the public and shall determine, *in consultation with the disputing parties*, the appropriate logistical arrangement'.[46] Accordingly, the transparency of the proceeding is largely subject to the law of the respondent state. This conclusion can also be made from examining Article 9.17.4 of the China-Australia FTA, which allows a respondent to reject disclosure or allow access to information according to Article 16.1 (Disclosure and Confidentiality of Information) or Article 16.3 (Security Exceptions).[47]

Moreover, based on its law, an investment host state can require an investor to disclose information relevant to investment, which may include personal data. For example, both the CPTPP and the USMCA provide that, notwithstanding national treatment and most-favoured-nation treatment, 'a Party may require an investor of another Party or its covered investment to provide information concerning that investment solely for informational or statistical purposes'.[48] Here, 'a Party' refers to the investment host state. Although the CPTPP and the USMCA require the investment host state to protect the information released by the investor, this does not mean that the host state is prevented from obtaining or disclosing information according to its law in an equitable and good-faith manner.[49]

The data protection law of the investor's home state, nevertheless, may be applied according to three treaty provisions. The first is the Governing Law provision in the investment chapters of the CPTPP and China-Australia FTA, which provides that the tribunal shall decide the dispute according to the pertinent investment

[43] CPTPP, *supra* note 16, Art. 9.24.3 (emphasis added).

[44] For data subject access requests, see Allen & Overy, *GDPR for Litigators* (2019), at 6, available at www.allenovery.com/en-gb/global/news-and-insights/publications/gdpr-for-litigators-2019.

[45] CPTPP, *supra* note 16, Art. 9.24.5; USMCA, *supra* note 15, Art. 14.D.8.5 (emphasis added).

[46] China-Australia FTA, *supra* note 17, Art. 9.17.3 (emphasis added).

[47] *Ibid.*, Art. 9.17.4.

[48] CPTPP, *supra* note 16, Art. 9.14.2; USMCA, *supra* note 15, Art. 14.13.2.

[49] CPTPP, *supra* note 16, Art. 9.14.2; USMCA, *supra* note 15, Art. 14.13.2.

agreement and the treaty that an arbitration is pursuant to; so the law of the investor home state will apply if the agreement requires.[50] However, if in the investment agreement, the choice of law has not been specified or otherwise agreed, both the CPTPP and the China-Australia FTA require the tribunal to consider the law of the respondent state.[51] Second, the provision for Disclosure of Information allows a member state not to disclose information according to its law, public interest, etc.[52] Nevertheless, this provision provides for the application of the laws of both the investor's home state and the respondent state, so it does not help the tribunal to resolve conflicts (if any) between the two laws. Last but not least, Article 32.8 of the USMCA regulates personal information protection. It includes key principles such as limitation on collection, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation and accountability.[53] However, this provision also equally applies to both the investor's home state and the respondent state. Therefore, although allowing the application of the law of the investor's home state, the USMCA, CPTPP and China-Australia FTA generally provide more possibilities to apply the law (including on personal data protection) of the respondent state.

Disputes on personal data protection are procedural issues. According to the 2013 UNCITRAL Arbitration Rules, an arbitral tribunal may conduct the arbitration as it considers appropriate provided that the parties are treated equally.[54] Article 47 of the ICSID Convention also provides that tribunals may recommend any provisional measures which should be taken to preserve the respective rights of each party.[55] Therefore, arbitral tribunals have the power to determine the conduct of proceedings regarding issues of personal data protection.[56] The critical issue is whether data protection laws (especially the GDPR) should have a restricting effect on the freedom of arbitral tribunals to decide whether or not to disclose certain information and documents. The answer first depends on whether the GDPR would be applied. If the respondent state is

[50] CPTPP, *supra* note 16, Art. 9.25; China-Australia FTA, *supra* note 17, Art. 9.18.

[51] E.g. China-Australia FTA, *supra* note 17, Art. 9.18; CPTPP, *supra* note 16, Art. 9.25.2.b(i) (requiring the application of the law of the respondent, including its rules on conflict of laws, and such rules of international law as may be applicable).

[52] E.g. CPTPP, *supra* note 16, Art. 29.7; China-Australia FTA, *supra* note 17, Art. 16.1; USMCA, *supra* note 15, Art. 32.7; EVIPA, *supra* note 18, Art. 4.12.

[53] USMCA, *supra* note 15, Art. 32.8.3.

[54] UNCITRAL Arbitration Rules (2013 UNCITRAL Arbitration Rules), GA Res. 68/109, 16 December 2013, Art. 17.1. The 2013 UNCITRAL Rules remain unchanged from the UNCITRAL Arbitration Rules (2010 UNCITRAL Arbitration Rules), GA Res. 65/22, 6 December 2010, except for the addition of Art. 1, para. 4; both sets of rules are available at https://uncitral.un.org/en/texts/arbitration/contractualtexts/arbitration.

[55] Convention on the Settlement of Investment Disputes between States and Nationals of Other States (ICSID Convention) 1965, 575 UNTS 159, Art. 47.

[56] E.g. CPTPP, *supra* note 16, Art. 9.24. Nevertheless, depending on the treaty that an arbitration is pursuant to, personal data protection issues may ultimately have to be decided by a body other than an arbitral tribunal. See, e.g., US-Korea FTA, *supra* note 37, Art. 11.21(4) (providing a review mechanism for the tribunal's decisions on data protection issues).

not an EU member state, this state may deviate from the GDPR due to various grounds ascribed in the treaty that the arbitration is pursuant to.[57] Second, the tribunal should conduct a balancing test to avoid a party to the arbitration using local data protection laws to reject access to fundamental documents and completely shifting the power in arbitral proceedings. In *Giovanna A. Beccara and Others v. Argentina,* when deciding whether Argentina should have access to a database containing the Italian Claimants' personal information, the tribunal held that:

> Thus, in accordance with Article 44 of the ICSID Convention and Rule 19 of the ICSID Arbitration Rules, unless there exist an agreement of the Parties on the issue of confidentiality/transparency, the Tribunal shall decide on the matter on a case by case basis and, instead of tending towards imposing a general rule in favour or against confidentiality, try to achieve a solution that balances the general interest for transparency with specific interests for confidentiality of certain information and/or documents.[58]

Consequently, the tribunal imposed certain Italian Privacy Code based restrictions on Argentina's access to the database. Besides the general interest for transparency with specific interests for confidentiality, when conducting the balancing test, a tribunal may also consider whether a local data protection law is applied in an equitable and good-faith manner.[59] Other factors may also include issues such as whether a law provides non-discriminatory treatment to the protection of personal information of data subjects from a foreign country[60] and whether a law complies with principles and guidelines of relevant international bodies (for example, the Asia-Pacific Economic Cooperation's Privacy Framework and the Organisation for Economic Co-operation and Development's 2013 Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data).[61]

C *Arbitration Rules*

In arbitration law, confidentiality means the obligation not to disclose documents (for example, decisions and pleadings) used for the purpose of arbitration to any third parties.[62] It usually encompasses access to documents, the publication of awards, orders and decisions of the tribunal, open hearings and the attendance at, or observance of, the hearings by third parties (*amicus curiae*).[63] International commercial arbitration should

[57] These grounds, in the cases of the CPTPP, the USMCA and the China-Australia FTA, are discussed in notes 47–51 above and accompanying texts.

[58] ICSID, *Giovanna A. Beccara and Others v. Argentina*, 27 January 2010, ICSID Case no. ARB/07/5, para. 73.

[59] CPTPP, *supra* note 16, Art. 9.14.2; USMCA, *supra* note 15, Art. 14.13.2.

[60] USMCA, *supra* note 15, Art. 32.9.

[61] USMCA, *supra* note 15, Arts 32.8.6, 32.8.2. APEC Privacy Framework, *supra* note 1; OECD 2013 Recommendation, *supra* note 1.

[62] Saravanan and Subramanian, 'Transparency and Confidentiality Requirements in Investment Treaty Arbitration', 5(4) *Brics Law Journal* (2018) 114, at 116; Michael Collins, 'Privacy and Confidentiality in Arbitration Proceedings' (1995) 30(1) *Texas International Law Journal* 121, 126.

[63] Saravanan and Subramanian, *supra* note 62, at 118–119; Clifford and Scogings, *supra* note 27, at 392–393.

generally be kept confidential unless the parties agree otherwise.[64] Different from commercial arbitration, without any agreement between the parties on this issue, 'there is no provision imposing a general duty of confidentiality in ICSID arbitration, whether in the ICSID Convention, any of the applicable Rules or otherwise. Equally, however, there is no provision imposing a general rule of transparency or non-confidentiality in any of these sources'.[65] Neither the 1976 nor the 2010 United Nations Commission on International Trade Law's (UNCITRAL) Arbitration Rules contains provisions on confidentiality or transparency, but some of the rules implicate the application of a local data protection law.[66] For example, the 1976 Arbitration Rules limit the publication of the proceedings to the award and, even then, only with the consent of both parties.[67] The 2010 Arbitration Rules provide that an award may also be made public when this is required by a party because of a legal duty or to protect or pursue a legal right.[68] The 'legal duty' can cover a data controller's obligation to provide a data subject with access to his or her data. The 'legal right' may refer to the right to protect personal data depending on the specific case scenario. Moreover, Article 17 of the 2010 Arbitration Rules requires all communications to the tribunal by one party to be communicated by that party to all other parties.[69] It also provides that such communications shall be made at the same time unless otherwise permitted by the tribunal if it may do so under applicable law.[70] This requirement means that, if an applicable data protection law requires, the tribunal may order redaction of protected personal information in the communications before transmitting them to the other parties.

On the subject of the hearing, Rule 32 of the ICSID Arbitration Rules allows the tribunal, unless either party objects, to allow other persons (who are not the parties, their agents, counsels and advocates, witnesses and experts during their testimony or officers of the Tribunal) to attend the hearings.[71] Modern investment treaties have adopted higher obligatory requirements on transparency. For example, the 2001 Notes of Interpretation of Certain Chapter 11 Provisions by the North American Free Trade Agreement's (NAFTA) Free Trade Commission negates a general duty of confidentiality in Chapter 11 proceedings and states that nothing precludes the parties from providing public access to documents relating thereto.[72] Article 9.24.2 of the

64 Amaalanczuk, 'Confidentiality and Third-Party Participation in Arbitration Proceedings under Bilateral Investment Treaties', 1(2) *Contemporary Asia Arbitration Journal* (2008) 183, at 186.

65 ICSID, *Biwater Gauff (Tanzania) Limited v. United Republic of Ranzania*, 29 September 2006, ICSID Case no. ARB/05/22, para. 121; ICSID, *Giovanna A. Beccara and Others v. Argentina*, 27 January 2010, ICSID Case no. ARB/07/5, para. 73 (holding that '[i]n conclusion, the Tribunal deems that the ICSID Convention and Arbitration Rules do not comprehensively cover the question of the confidentiality/transparency of the proceedings').

66 2010 UNCITRAL Arbitration Rules, *supra* note 54.

67 1976 UNCITRAL Arbitration Rules, GA Res. 31/98, 15 December 1976, Art. 32.5.

68 2010 UNCITRAL Arbitration Rules, *supra* note 54, Art. 34.5.

69 *Ibid*, Art. 17.4.

70 *Ibid*.

71 ICSID Rules of Procedure for Arbitration Proceedings (ICSID Arbitration Rules), April 2006, Rule 32.

72 NAFTA Free Trade Commission, Notes of Interpretation of Certain Chapter 11 Provisions (NAFTA Notes of Interpretation), 31 July 2001. North American Free Trade Agreement (NAFTA) 1992, 32 ILM 289, 309 (1993).

CPTPP provides that the tribunal shall conduct hearings that are open to the public.[73] Regarding the publication of documents, Regulation 22 of the International Centre for Settlement of Investment Disputes' (ICSID) Administrative and Financial Regulations provides that, when both parties to the proceeding consent to the publication, the secretary-general shall appropriately publish arbitral awards and the minutes and other records of proceedings.[74] The CPTPP goes further by specifying a comprehensive scope of publication and restricting the circumstances in which parties may object to the publication.[75] Nevertheless, the tribunal must take measures to protect proprietary, privileged or protected information.[76]

An important measure that a tribunal may take is to issue confidential orders to protect personal data.[77] However, the confidentiality obligation in traditional investment arbitration law is not the same as the privacy obligation in the data protection regime in (at least) three ways: subjects, objects and contents. Consequently, personal data protection expands the scope of protecting confidential information in investment arbitration.

1 Subjects

In an investment arbitration, the subjects to fulfil the confidentiality obligation are arbitral participants and arbitration institutions (for example, the ICSID Centre, the Permanent Court of Arbitration [PCA]). The extent of the confidentiality obligation as well as to whom it applies are determined pursuant to investment treaties and arbitration rules. For instance, the ICSID Arbitration Rules regulate the confidentiality obligations of the centre and of the arbitrators but not of the parties.[78] In practice, some authorities, such as in *Amco v. Indonesia*, confirm that the ICSID Convention and the Arbitration Rules do not prevent the parties from revealing their case.[79] Thus, the parties are in principle free to publish documents or awards unless they have explicitly agreed upon confidentiality under the ICSID regime.[80] In the context of NAFTA, it is

[73] CPTPP, *supra* note 16, Art. 9.24.2.

[74] ICSID Administrative and Financial Regulations, January 2003, ICSID/15/Rev. 1, Regulation 22.

[75] The CPTPP, *supra* note 16, Art. 9.24, requires publication of the notice of intent, the notice of arbitration, pleadings, memorials and briefs, minutes or transcripts of hearings of the tribunal, orders and awards and decisions of the tribunal. Art. 9.24 also provides that the respondent can object to publication based on Art. 29.2 (Security Exceptions) or Art. 29.7 (Disclosure of Information) and that protected information shall be protected from disclosure.

[76] ICSID Arbitration Rules, *supra* note 71, Rule 32; CPTPP, *supra* note 16, Art. 9.24.2.

[77] Federal Court of Canada, *Appleton & Associates v. Barry Appleton, the Clerk of the Privy Council Office*, 19 June 2007, Case no. T-579-06, paras 16, 23 (the Federal Court of Canada found that documents containing personal information should not be released to a third party given a confidentiality order issued by the arbitral tribunal in *UPS v. Canada*, ICSID Case No. UNCT/02/).

[78] The confidentiality obligations of the International Centre for Settlement of Investment Disputes (ICSID) and arbitrators are prescribed in ICSID Arbitration Rules, *supra* note 71, Rules 48(4)–(5), 6(2) respectively.

[79] ICSID, *Amco Asia Corporation and others v. Republic of Indonesia – Decision on Provisional Measures*, 9 December 1983, ICSID Case no. ARB/81/1, at 410, 412, para. 2. ICSID Convention, *supra* note 55.

[80] Knahr and Reinisch, 'Transparency versus Confidentiality in International Investment Arbitration: The Biwater Gauff Compromise', 6 *Law and Practice of International Courts and Tribunals* (2007) 97, at 100–101.

easier to access documents through parties because the NAFTA tribunals 'have generally concluded that parties therefore remained free to publicly discuss cases to which they were parties'.[81]

In the context of the data protection regime of the GDPR, the subjects of confidentiality obligations relating to personal data are 'controller'[82] and 'processor'.[83] According to Article 2 of the GDPR, three components constitute a 'controller': (i) a natural or legal person, public authority, agency or other bodies (ii) that alone or jointly with others (iii) determines the purposes and means of data processing.[84] Processor means a natural person or an entity that processes personal data on behalf of the controller.[85] Under the GDPR, both the controller and the processor have privacy obligations. For example, in *Tennant Energy v. Canada*, the claimant submitted that the GDPR should be applied because the arbitrators and the PCA were allegedly 'processors'.[86] This was because Sir Daniel Bethlehem, QC, a United Kingdom (UK) national, processed personal data when he decided the case, and the PCA processed data when it collected, stored or transmitted the data.[87] Parties, party witnesses and experts are the joint controllers of data under the GDPR.[88]

Importantly, not every local data protection law imposes privacy obligations based on the roles of 'controller' and 'processor'. In the PIPA, even if a party is neither a controller nor a processor, it may be subject to a privacy obligation. In *Elliott*, the tribunal noted that the PIPA does not merely regulate personal information controllers who process personal information for the purposes of operating personal information files.[89] The PIPA also protects certain personal information that is not under the control or in the possession of a personal information controller.[90] Thus, it was held that whether the Ministry of Justice, or Korea more broadly, was an information controller was irrelevant to the case.[91] Overall, what is clear is that the subjects of a privacy obligation in a data protection regime vary according to the applicable law.

2 Objects

Objects are different in the confidentiality obligation under traditional investment arbitration law and the privacy obligation in the data protection domain. Traditionally, the object of confidentiality obligation in investment arbitration is confidential business

[81] *Ibid.*, at 101.
[82] GDPR, *supra* note 1, Art. 4(7).
[83] *Ibid.*, Art. 4(8).
[84] P. Voigt and A. von dem Bussche, *Scope of Application of the GDPR* (2017), at 18–20.
[85] GDPR, *supra* note 1, Art. 4(8).
[86] PCA, *Tennant Energy, LLC (USA) v. Government of Canada*, PCA Case no 2018–54. Claimant Email to the Tribunal re Application of the EU GDPR, Doc. UN-0195-10, 17 April 2019.
[87] *Ibid.*
[88] *Ibid.*
[89] *Elliott*, *supra* note 36, Procedural Order no. 4, para. 38.
[90] *Ibid.* That information was defined as 'information relating to a living individual that makes it possible to identify the individual by his/her full name'.
[91] *Ibid.*, para. 37.

information, intellectual property information, information that is privileged or otherwise protected from disclosure under a party's domestic law or information that a party must withhold pursuant to the relevant arbitral rules as applied.[92] In contrast, the object of the privacy obligation in the data protection domain is personal information.[93] Typically, it is defined as information of any nature whatsoever that, standing alone or as linked to other information, could be used to identify an individual.[94] Examples would include formalized personal data such as name, date of birth, residential address and the employment history of a data subject and would also cover automated data such as Internet protocol addresses and cookie identifiers according to applicable data protection regulations.[95] Nevertheless, personal data may overlap with confidential information in investment arbitration. For example, a list of the names of potential buyers may be considered as both a confidential business secret and personal data.

3 Contents

The confidentiality obligation under traditional investment arbitration law focuses on the accessibility and security of the confidential information. For example, interactions between an administering institution and the parties, tribunal deliberation and draft awards are generally intended to remain private and confidential.[96] If the parties and tribunal decide not to provide access for third parties to the hearing and the documents, the relevant information must be kept in an appropriate, secure manner for a period of time as is legitimate. If arbitration involves intellectual property or trade secrets and one disputing party does not want such information to be provided to the other disputing party or even to the tribunal, some arbitration rules provide highly confidential mechanisms to address these issues.[97] Whether the information is accurate, whether it is obtained lawfully and whether it is analysed properly are not included in the confidentiality obligation, although they are relevant to the arbitration.

Comparatively, the privacy obligation in the data protection domain has a broader scope. For example, the GDPR requires that (i) data is processed[98] lawfully, fairly and

92 See, e.g., NAFTA Notes of Interpretation, *supra* note 72, para. 2(b).

93 See, e.g., GDPR, *supra* note 1, Art. 1.

94 See the definition of personal data in note 2 above.

95 Trakman, Zeller and Walters, 'Is International Arbitration Prudent When Dealing with Personal Data Challenges?', 17(2) *Transnational Dispute Management* (2020) 1, at 10.

96 Under NAFTA, hearings (unless the disputing parties decide otherwise), written submissions, witness statements and responses to tribunal questions will be made public as soon as possible after the documents are filed. The current ICSID Arbitration Rules do not prohibit the parties to an ICSID arbitration from disclosing memorials, briefs and other submissions in the arbitration. The UNCITRAL Rules on Transparency provide broader scope of transparency. However, none of the three covers tribunal deliberation, draft awards, etc. See Gary B. Born, *International Commercial Arbitration* (Wolters Kluwer Law International 2020), §20.11 Confidentialty in Investor-State Arbitration.

97 E.g. World Intellectual Property Organization, Arbitration Rules, 1 January 2020, Arts 75–78, available at www.wipo.int/amc/en/arbitration/rules/index.html#conf2 (last visited 9 June 2021).

98 See, e.g., GDPR, *supra* note 1, Art. 5(1)(f). Notably, the GDPR comprehensively defines 'processing' as including but not limited to collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use and disclosure (see Art. 4(2)).

transparently; (ii) data is collected for specified, explicit and legitimate purposes; (iii) data is adequate, relevant and limited to what is necessary; (iv) data should be accurate and kept up to date; (v) data is kept in a form that permits identification of data subjects for no longer than necessary; and (vi) data is processed in an appropriately secure manner.[99] Moreover, under traditional investment arbitration law, the level of the permissibility of publication and the distribution of documents may be determined by the categories of documents (awards, minutes of hearings, witness statements, submissions by parties and so on) and by whether the arbitral proceeding is pending or concluded.[100] However, such considerations are irrelevant to the protection of personal data. The privacy of personal data should be maintained regardless of both the categories of the relevant documents and whether the arbitration has yet to commence, is ongoing or has finished.

3 Mandatory Application and Exemption

This section goes beyond the consensual application of local data protection laws. It asks whether, due to its nature as a mandatory law, a local data protection law should be applied to investment arbitration whenever the data processing falls within the material and territorial scope of the law. The section first analyses the mandatory nature of a local data protection law using the GDPR as an example. It then argues that the mandatory application of a local data protection law can be exempted because of the privileges and immunities accorded by public international law.

A *Local Data Protection Laws as Mandatory Laws*

The GDPR is applicable to investment arbitrations because Recital 20 of the GDPR provides that the GDPR applies to the activities of courts and other judicial authorities.[101] These activities include arbitration.[102] Recital 20 contains an exemption providing that the competence of the data supervisory authorities does not cover the processing of personal data when courts are acting in their judicial capacity in order to safeguard the independence of the judiciary in the performance of their judicial tasks, including decision-making.[103] However, this exemption does not extend to arbitration.[104] In addition, although Recital 91 of the GDPR exempts lawyers from conducting a data protection impact assessment, other obligations under the GDPR are still applicable.[105]

[99] *Ibid.*, Art. 5.1.

[100] Knahr and Reinisch, *supra* note 80, at 113–116.

[101] GDPR, *supra* note 1, Recital 20.

[102] M. Zahariev, 'GDPR Issues in Commercial Arbitration and How to Mitigate Them', *Kluwer Arbitration Blog* (7 September 2019), available at http://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate-them/.

[103] Trakman, Zeller and Walters, *supra* note 95, at 4–5.

[104] Paisley, 'It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration', 41(4) *Fordham International Law Journal* (2018) 841, at 857; Zahariev, 'Mission(Im)Possible: Where GDPR Meets Commercial Arbitration', *Austrian Yearbook on International Arbitration* (2020) 3, at 5–6.

[105] GDPR, *supra* note 1, Recital 91.

The fact that the GDPR applies to an arbitration generally does not necessarily mean that it should be applied to a particular investment arbitration. Recital 16 of the GDPR provides that it does not apply to the issues of protection of personal data 'related to activities which fall outside the scope of Union law, such as activities concerning national security'.[106] It also does not apply to the processing of personal data by member states carrying out activities of common foreign and security policy of the Union.[107] Article 2.2(a) of the GDPR describes its material scope: 'This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law'.[108] Article 3 of the GDPR delimitates its territorial scope. The GDPR applies if personal data is processed in the context of the activities of the EU establishment, in connection with the offering of products and services to data subjects in the EU or in the context of monitoring the behaviour of data subjects in the EU.[109] Recital 22 states that an establishment 'implies the effective and real exercise of activity through stable arrangements'.[110]

The GDPR should apply to an investment arbitration pursuant to a treaty where the EU or one or more of its member states are parties.[111] However, it is disputable whether the GDPR should be applied to an investment arbitration brought according to a treaty to which neither the EU nor its member states is a party. In *Tennant*, the tribunal considered whether an arbitrator's domicile in the UK would lead to the application of the GDPR.[112] Tennant was a US company, the arbitration was brought pursuant to NAFTA and the applicable procedural law was the 1976 UNCITRAL Arbitration Rules.[113] The tribunal found that the GDPR was inapplicable because the arbitration was carried out under NAFTA Chapter 11, a treaty to which neither the EU nor its member states was a party, and the arbitration was thus not in the material scope of the GDPR.[114] Nevertheless, in *VQ v. Land Hessen*, the Court of Justice of the European Union (CJEU) held that it was not appropriate to interpret the expression 'activity which falls outside the scope of Union law' in Article 2(2)a of the GDPR as 'having a meaning which would require it to be determined in each individual case whether the specific activity at issue directly affected freedom of movement between Member States'.[115] Because Article 2(2)a is an exception to the very wide scope of application of the GDPR, it must be interpreted restrictively.[116] The CJEU held that 'activity which falls outside the scope

[106] *Ibid.*, Recital 16.

[107] *Ibid.*

[108] Other exceptions under GDPR, *ibid.*, Art. 2.2(a), include common European security and defence policy, purely personal or household activities and criminal activities.

[109] *Ibid.*, Art. 3.

[110] *Ibid.*, Recital 22.

[111] See section 2.B.

[112] *Tennant*, *supra* note 86. *Tennant* was decided before Brexit.

[113] The 1976 UNCITRAL Arbitration Rules, *supra* note 67, except as modified by the provisions of NAFTA, *supra* note 72, Section B of Chapter 11, Art. 1120(2).

[114] *Tennant*, *supra* note 86, tribunal's communication to the parties, 24 June 2019. Notably, the publicly available version of the email sent by the tribunal has been partially redacted and does not reveal much of the tribunal's analysis.

[115] Case C-272/19, *VQ v. Land Hessen* (EU:C:2020:535), para. 66.

[116] *Ibid.*, para. 67.

of Union law' under Article 2(2)a of the GDPR should be limited to activities expressly listed in Article 3(2) of Commission Directive (EC) 96/46 (that is, activities provided for by Titles V and VI of the Treaty on European Union and data processing operations concerning public security, defence, State security and activities in areas of criminal law) or activities that can be similarly classified.[117] In the context of *Land Hessen*, the tribunal's decision in *Tennant* that the investment arbitration was not subject to the GDPR because neither the EU nor its member states was a party to NAFTA is questionable. It is not evident that investment arbitration or the issue of NAFTA membership would fall within the listed activities in Article 3(2) of Commission Directive 96/46 or could be classified in the same category as those activities. Notably, *Tennant* was decided before *Land Hessen* was rendered. Therefore, for post-*Land Hessen* cases, investment arbitration tribunals may have to narrowly define the exceptions under Article 2(2) of the GDPR. Consequently, the GDPR may be applied to an arbitration involving a matter that is not itself subject to EU law.

Moreover, in *Tennant*, even if the GDPR would not apply, the tribunal failed to consider whether the UK Data Protection Act 2018 (DPA 2018) would apply.[118] The DPA 2018 establishes the data protection framework in the UK. Part 2, Chapter 2, of the DPA 2018 applies to the majority of personal data processing in the UK.[119] It supplements and tailors the GDPR and must be read together with it.[120] Part 2, Chapter 3 of the DPA 2018 applies to the processing of personal data in the course of an activity that is outside the scope of EU law.[121] However, the protection regime created by Chapter 3 is broadly equivalent to the GDPR.[122] Therefore, in any case, even if the GDPR would not apply, the relevant local data protection law within the EU member state might. The local data protection law probably regulates data protection in a way that is equivalent to the GDPR. Therefore, tribunals still have to consider the messy conflict-of-laws situation.

B *Exemption by Privileges and Immunities under Public International Law*

A possible way to exclude the mandatory application of a local data protection law and resolve the messy conflict-of-laws situation is to invoke privileges and immunities

[117] *Ibid.*, paras 69–70. Council Directive (EC) 95/46, OJ 2016 L 119. Treaty on European Union, OJ 2010 C 83/13.

[118] Data Protection Act 2018 (DPA 2018), c. 12, available at www.legislation.gov.uk/ukpga/2018/12/contents/enacted, last visited 9 June 2021. The GDPR has direct effect in United Kingdom (UK) law and automatically applies in the UK until the end of the Brexit transition period. After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context. See Information Commissioner's Office, About the DPA 2018, available at https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/, last visited 9 June 2021.

[119] DPA 2018, *supra* note 118, ss 6–20.

[120] *Ibid.*

[121] *Ibid.*, ss 21(1)(a).

[122] *Ibid.*, ss 4(3)(b).

under public international law.[123] Privileges and immunities aim to provide the guarantee for an international organization and its officials, a sovereign state and its staff with diplomatic status and other personnel to independently perform their duties and fulfil their obligations in order to achieve the goal of that international organization or the state.[124] For the purposes of this article, 'privileges' refers to the non-application of a local data protection law and 'immunities' means jurisdictional immunity – namely the exemption from any process of violating the local law.[125] They have the same negating effect in the sense that the local data protection law has no impact on an investment arbitration and its participants.[126]

The privileges and immunities under public international law can exempt the mandatory application of a local data protection law.[127] The ICJ analysed 'immunities from legal process of every kind in respect of words spoken or written' in a binding advisory opinion on the *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights* (*Cumaraswamy*).[128] This case concerned an interview given by a Malaysian jurist (who was appointed a special rapporteur by the United Nations) to a magazine not only published in the UK but also circulated in Malaysia. The special rapporteur commented on certain proceedings that had been brought (and concluded) in Malaysian courts. Consequently, several individuals and entities filed suits in Malaysia against the special rapporteur for slander.[129] The ICJ confirmed the secretary-general's finding that Mr. Cumaraswamy, in the words quoted in the article, was acting in the course of the performance of his mission and was entitled to immunity from legal process in Malaysia.[130]

Like the law of slander in *Cumaraswamy*, personal data protection laws vary from jurisdiction to jurisdiction because these laws reflect the different concepts of privacy in each state.[131] In *Google LLC, Successor in Law to Google v. Commission nationale de*

[123] For detailed discussion of how privileges and immunities under public international law may exempt an investment arbitration from complying with a local data protection law, see Huang and Xie, *supra* note 10, at 182–195.

[124] Reinisch, 'Privileges and Immunities', in J.K. Cogan, I. Hurd and I. Johnstone (eds), *The Oxford Handbook of International Organizations* (2016) 1048, at 1050–1052.

[125] E.C. Okeke, *Jurisdictional Immunities of States and International Organizations* (2018), at 4 (defining 'jurisdictional immunity' as 'immunity from legal or judicial process' that 'bars a national court from subjecting certain legal persons to judicial process or adjudicating their legal relations').

[126] *Ibid.*, at 5 (arguing that 'the issue of immunity … is a derogation from a national court's jurisdiction that renders domestic law unenforceable').

[127] The consensual application of a local data protection law discussed in section 2 cannot be exempted by the privileges and immunities under public international law because the local law is chosen by the parties.

[128] *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights*, Advisory Opinion, 29 April 1999, ICJ Reports (1999) 62.

[129] *Ibid.*, para. 6.

[130] *Ibid.*, para. 59.

[131] For the differences between the USA's and the EU's concepts of personal data protection, see McGeveran, 'Friending the Privacy Regulators', 58 *Arizona Law Review* (2016) 959, at 961; Peltz-Steele, 'The New American Privacy', 44 *Georgetown Journal of International Law* (2013) 365, at 372; see also Schulhofer, 'An International Right to Privacy? Be Careful What You Wish For', 14 *IJCL* (2016) 238, at 238–261.

l'informatique et des libertés (CNIL),[132] the CJEU held that it should respect that other states likely exercised a different balance between the right to privacy and the freedom of information of Internet users.[133] Personal data protection laws are applied as mandatory laws by some states for purposes such as censorship and national security.[134] Therefore, 'immunities from legal process of every kind in respect of words spoken or written', as held in *Cumaraswamy*, should include local data protection laws.

Regarding investment arbitration conducted under the auspices of ICSID, Articles 21 (a) and 22 of the ICSID Convention grant immunity to arbitrators and other arbitral participants from legal process with respect to acts performed by them in the exercise of their functions, except when the ICSID Centre waives this immunity.[135] Both provisions aim to prevent the interruption of local laws in the proceedings.[136] The immunity that they grant should include the exemption from legal processes of every kind under a local data protection law with respect to words spoken or written when the arbitrator and other arbitral participants perform their duties.[137]

In the PCA, investment arbitrations are generally not brought pursuant to the two founding Hague Conventions.[138] Nevertheless, the privileges and immunities of arbitral participants in investment arbitration conducted under the auspices of the PCA can be found in the host country agreements that the PCA has concluded with Argentina, Chile, China (in relation to the Hong Kong Special Administrative Region), Costa Rica, Djibouti, India, Ireland, Malaysia, Mauritius, Paraguay, Portugal, Singapore, South Africa, Uruguay and Vietnam.[139] According to those host country agreements,[140]

[132] Case C-507/17, *Google LLC, Successor in Law to Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)* (EU:C:2019:772).

[133] *Ibid.*, paras 59–60.

[134] For the mandatory nature of personal data protection law in the USA, the EU and China, see Huang, *supra* note 6, at 1296–1298. For a case examining personal data used for digital surveillance and national security in the USA, see Case C-311/18, *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (EU:C:2020:559).

[135] ICSID Convention, *supra* note 55, Arts 21(a), 22; C.H. Schreuer *et al.* (eds), *The ICSID Convention: A Commentary* (2010), at 62–66.

[136] Schreuer, *supra* note 135, at 65. In *Libananco v. Turkey*, the tribunal applied the ICSID Convention, *supra* note 55, Arts 21, 22, to the claim brought by the claimant that Turkey was keeping Libananco's legal representative and potential witnesses under surveillance and that there had been interception of the email communications of Libananco's counsel in the arbitration. ICSID, *Libananco Holdings Co. Limited v. Turkey – Decision on Preliminary Issues*, 23 June 2008, ICSID Case no. ARB/06/8, paras 72, 82.

[137] *Ibid.*

[138] The PCA was established by the Hague Convention for the Pacific Settlement of International Disputes 1899, 1 AJIL 103 (1907), which was replaced by the Hague Convention for the Pacific Settlement of International Disputes 1907, 2 AJIL Supp. (1908), available at https://pca-cpa.org/wp-content/uploads/sites/6/2016/01/1907-Convention-for-the-Pacific-Settlement-of-International-Disputes.pdf.

[139] PCA, Annual Report 2019, Annual Report no. 119 (2019), at 42; see also Host Country Agreements, available at https://pca-cpa.org/en/relations/host-country-agreements/.

[140] E.g. Headquarters Agreement between PCA and the Netherlands (Hague Headquarters Agreement), 30 March 1999; the International Organizations (Privileges and Immunities) (Permanent Court of Arbitration) Order (Hong Kong) (Hong Kong Order), Cap 558 I, s. 3. This order was issued according to the Host Country Agreement between the Government of People's Republic of China and the Permanent Court of Arbitration on the Conduct of Dispute Settlement Proceedings in the Hong Kong Special Administrative Region of the People's Republic of China, 4 January 2015.

arbitrators[141] and other arbitral participants[142] enjoy immunity from legal processes of every kind with respect to the words spoken or written and the acts performed by them in the course of the discharge of their duties or in the course of their participation in the PCA proceedings or PCA meetings.[143] In conclusion, investment arbitration participants may enjoy privileges and immunities from a local data protection law but not always. For example, in the case of the PCA, the host country agreements provide privileges and immunities only from the laws of the 15 host countries.

4 What Effects Will the Application of Local Data Protection Laws Have on General Investment Arbitration?

This section focuses on four normative questions: how local data protection laws would influence the trend towards transparency in investment arbitration brought pursuant to modern investment treaties (section A); whether data protection in investment arbitration would disturb the balance of power towards one of the parties (section B); whether it is good to have multiple data protection laws directly applicable in an investment arbitration proceeding (section C); and whether the so-called Brussels Effect may take hold in investment arbitration (section D).

A *Transparency versus Privacy*

There exists in modern investment treaties a widely acknowledged trend towards transparency.[144] The questions are how data protection laws would influence such a trend and whether they would prompt tribunals to reverse transparency requests and return to more secretive proceedings. These questions should be analysed in the context of the Mauritius Convention and the UNCITRAL Rules on Transparency.[145] This

[141] Arbitrators are included in the definition of the PCA adjudicator in the host country agreements. E.g. in the Hague Headquarters Agreement, *supra* note 140, Art. 1.8, PCA adjudicator means 'any arbitrator, mediator, conciliator, or member of an international commission of inquiry taking part in a hearing, meeting, or other activity in relation to PCA Proceedings'.

[142] Both the Hong Kong Order, *supra* note 140, Art. 1, and the Hague Headquarters Agreement, *supra* note 140, Art. 1.9, distinguish arbitrators from 'participant in proceedings', which refers to 'any counsel, party, agent, or other party representative, witness, expert, as well as any interpreter, translator, or court reporter taking part in a hearing, meeting, or other activity in relation to PCA Proceedings' held in Hong Kong or at the Hague.

[143] For arbitrators, see the Hong Kong Order, *supra* note 140, Art. 6.1.(a), and Hague Headquarters Agreement, *supra* note 140, Art. 9.1. For other arbitral participants, see Hong Kong Order, Art. 8.1(a); Hague Headquarters Agreement, Art. 9.2. B.W. Daly, E. Goriatcheva and H. Meighen, *A Guide to the PCA Arbitration Rules* (2014), at 62–63. The immunity period that other arbitral participants enjoy is shorter than that enjoyed by arbitrators, PCA officials and staff.

[144] See section 2.C.

[145] Mauritius Convention, *supra* note 3, Art. 2, provides the application of the Rules on Transparency, *supra* note 4.

is because they are the most prominent endorsement of the trend towards transparency. The former convention has been ratified by seven states, and the latter rules have been adopted in 61 investment treaties.[146] They aim to widely cover investment arbitrations. For an investment arbitration initiated pursuant to a treaty concluded on or after 1 April 2014 and the UNCITRAL Arbitration Rules, the Rules on Transparency will apply to the arbitration unless the parties to the treaty have agreed otherwise.[147] As for an investment arbitration brought pursuant to a treaty concluded before 1 April 2014, the Rules on Transparency may be applied when one of two criteria is met. First, the state of the claimant and the respondent state must have concluded the Mauritius Convention and express their consent to apply the Rules on Transparency to an investment arbitration initiated under any arbitration rules.[148] Second, the disputing parties in an arbitration agree to the application of the Rules on Transparency or the state of the claimant and the respondent state have agreed to their application.[149]

Compared to UNCITRAL's 1976 and 2010 Arbitration Rules and the ICSID Arbitration Rules, the Rules on Transparency set much higher obligations on the publication of documents and the provision of public access to hearings.[150] The Rules on Transparency also establish a Transparency Registry, which is a central, online database to publish information.[151] This database can make the general public's access to investment arbitration documents more convenient. The application of local data protection laws would not prompt tribunals to reverse transparency requests and return to more secretive proceedings for three reasons. First, the goals of transparency under the Mauritius Convention and the Rules on Transparency are to promote the good governance of states, corporate social responsibility, the legitimacy of investment arbitration, the evolution of consistent investment case law and general awareness as to the outcome of certain disputes that affect not only the parties to the dispute but also the public.[152] The protection of personal information does not contradict these goals.

Second, the interests underpinning secretive proceedings include procedural integrity, the risks of aggravating the dispute, the protection of governmental secrets and

[146] Seven states have ratified the Mauritius Convention up to 9 June 2021. See Status: United Nations Convention on Transparency in Treaty-based Investor-State Arbitration (New York, 2014), available at https://uncitral.un.org/en/texts/arbitration/conventions/transparency/status, last visited 9 June 2021. A list of investment treaties which contain the Rules on Transparency or provisions modelled on those rules can be found at https://uncitral.un.org/en/texts/arbitration/conventions/foreign_arbitral_awards/status.

[147] Rules on Transparency, *supra* note 4, Art. 1.1.

[148] Mauritius Convention, *supra* note 3, Arts 2, 3. The Rules on Transparency can also be applied if the respondent is a party to the Mauritius Convention and the claimant agrees to the application of the rules.

[149] Rules on Transparency, *supra* note 4, Art. 1.2.

[150] *Ibid.*, Arts 2, 3, 6.

[151] *Ibid.*, Art. 8. The repository is available at http://www.uncitral.org/transparency-registry/registry/index.jspx#country.

[152] Foden and Repousis, 'Giving Away Home Field Advantage: The Misguided Attack on Confidentiality in International Commercial Arbitration', 35(4) *AI* (2019) 401, at 402; Saravanan and Subramanian, *supra* note 62, at 114; Knahr and Reinisch, *supra* note 80, at 97, 110–111; J. Fry and Repousis, 'Towards a New World for Investor-State Arbitration through Transparency', 48 *New York University Journal of International Law and Politics* (2015) 795, at 804–807.

commercial confidential secrets and the maintenance of a good relationship between the investor and the respondent state.[153] At a doctrinal level, the protection of personal information does not aim to promote these interests. In the EU, the right to personal data protection is protected because it is a fundamental human right according to the European Convention for the Protection of Human Rights and Fundamental Freedoms and the European Charter for Fundamental Human Rights.[154] In the USA, the interests underlying the protection of personal information derive from personal liberty, restrictions on state action,[155] trust,[156] obscurity,[157] autonomy and so on.[158] Different from the EU and the USA, the Chinese legislature balances the protection of personal information with the need to develop the Chinese data industry and maintain public surveillance.[159] In arbitration practice, personal information such as name, gender and religion generally does not constitute government or commercial secrets.[160] Protecting personal information may not harm procedural integrity, aggravate the dispute or endanger the relationship between the investor and the respondent host state. Therefore, from both doctrinal and practical perspectives, protecting personal information, to a large extent, is not related to the promotion of secretive proceedings.

Third, personal information protection may benefit from the confidentiality exception under Article 7 of the Rules on Transparency.[161] Article 7 provides exceptions to transparency obligations: 'Confidential or protected information consists of ...

[153] Knahr and Reinisch, *supra* note 80, at 110.

[154] ECHR, *supra* note 29, Art. 8; EU Charter, *supra* note 29, Art. 8. For comments, see Cole and Fabbrini, *supra* note 13.

[155] *Roe v. Wade*, 410 U.S. 113, at 153 (1973). In *Whalen v. Roe*, although the US Supreme Court identified a general right to 'information privacy' in the Fourteenth Amendment, the Court upheld a New York statute requiring identification of physicians and patients in dangerous legitimate drug prescription records. *Whalen v. Roe*, 429 U.S. 589, from 605–606 (1977).

[156] 'Trust' is defined as a 'state of mind that enables its possessor to be willing to make herself vulnerable to another – that is, to rely on another despite a positive risk that the other will act in a way that can harm the truster'. Hill and O'Hara, 'A Cognitive Theory of Trust', 84 *Washington University Review* (2006) 1717, at 1724. In the data protection context, it means 'the willingness to become vulnerable to a person or organization by disclosing personal information'; Hartzog, 'Body Cameras and the Path to Redeem Privacy Law', 96(5) *North Carolina Law Review* (2018) 1257, at 1288.

[157] The concept of obscurity dates back to the *US Dept. of Justice v. Reporters Committee*, 489 U.S. 749 (1989). In this case, the US Supreme Court recognized a privacy interest in the 'practical obscurity' of information; the information was technically available to the public but was only accessible by spending a burdensome and unrealistic amount of time and effort.

[158] H.F. Nissenbaum, *Privacy in Context: Tecknology, Policy and the Integrity of Social Life* (2010), at 81–83; Cohen, 'Examined Lives: Informational Privacy and the Subject as Object', 52(5) *Stanford Law Review* (2000) 1373, at 1423–1426; Fried, 'Privacy', 77(3) *Yale Law Journal* (1968) 475, at 483.

[159] Xinbao, 'From Privacy to Personal Information: The Theory and System to Re-balance Interest', 3 *China Legal Science* [*Zhongguo Faxue*] (2015) 38, at 39 (indicating that the Chinese government, as the largest data controller in China, collects, processes, saves and uses personal information).

[160] E.g. in *Elliott*, the name of the then president of South Korea was protected as personal information but not considered a government secret. *Elliott*, *supra* note 36, Procedural Order no. 4, para. 25. For the differences between confidential information in traditional arbitration law and personal information in data protection law, see section 2.C.

[161] Rules on Transparency, *supra* note 4, Art. 7.1.

[i]nformation that is protected against being made available to the public, in the case of the information of the respondent State, under the law of the respondent State, and in the case of other information, under any law or rules determined by the arbitral tribunal to be applicable to the disclosure of such information'.[162] However, the Rules on Transparency do not allow a party to rely on a local data protection law to wholly undermine the transparency objectives of the rules.[163] Investment arbitration tribunals should balance the public interest in transparency, the data subjects' rights to protection of their personal information and the opposing party's interest in a fair and efficient resolution of the dispute.[164]

In conclusion, local data protection laws should not be considered as barriers to the trend towards transparency of investment arbitration and would not allow tribunals to return to more secretive arbitration proceedings.

B *Balance of Power*

Data protection in investment arbitration may disturb the balance of power between parties and shift it towards the respondent state. This is because the CPTPP, the USMCA and the China-Australia FTA provide more possibilities to apply the data protection law of the respondent state compared to other laws.[165] Moreover, Article 7 of the Rules on Transparency also explicitly provides that the information of the respondent state is to be protected according to the law of that state. This means that if the information is considered as protected personal information according to the law of the respondent state, but not according to the law of the investor's home state, the law of the former will prevail. It is unclear whether 'the information of the respondent state' is so broad as to include any personal information that the respondent state obtains as a data controller, which may cover personal information of foreign nationals. The narrower interpretation would be the literal one – that only information of the respondent state is included.

Like investment treaties, the GATS allows a respondent state to apply local data protection laws that are not inconsistent with its provisions.[166] However, to do so, and in contrast with investment treaties, the GATS imposes strict conditions on the respondent state. Article XIV of the GATS establishes a two-tier analysis.[167] First, the

[162] *Ibid.*, Art. 7.2.

[163] *Ibid.*, Art. 1.5.

[164] *Ibid.*, Art. 1.4.

[165] See section 2C.

[166] GATS, *supra* note 19, Art. XIV, provides that '[s]ubject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures … (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to … (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts'.

[167] WTO, *United States – Measures Affecting the Cross Border Supply of Gambling and Betting Services – Report of the Appellate Body* (*US – Gambling*), 20 April 2005, WT/DS285/AB/R, para. 292.

respondent state is required to (i) identify the data protection law that the protective measure is intended to secure compliance with; (ii) prove that that law is not in itself inconsistent with World Trade Organization (WTO) law; and (iii) prove that the protective measure is designed to secure compliance with that law.[168] Regarding whether the protective measure can secure compliance with the law of the respondent state, the tribunal should scrutinize the design of the measure sought to be justified.[169] If a protective measure can secure compliance, the tribunal should conduct the necessity test, which entails a more in-depth, holistic analysis of the relationship between the protective measure and the data protection law of the respondent state.[170] The necessity test requires a tribunal to consider (i) the importance of the objective pursued; (ii) the protective measure's contribution to that objective; and (iii) the trade restrictiveness of the measure.[171]

At the second level of the analysis, the respondent state must prove that the protective measure satisfies the requirements of the chapeau of Article XIV of the GATS.[172] The chapeau requires that the protection be applied in a manner that does not constitute 'arbitrary' or 'unjustifiable' discrimination or a 'disguised restriction on trade in services'.[173] It serves as a powerful tool in preventing the respondent state from unreasonably exercising the Article XIV exceptions and frustrating the rights accorded to other WTO member states.[174] In *Argentina – Financial Services*, the panel held:

> We recall that this objective is 'the ability … to have access to the information necessary to secure compliance with Argentina's laws and regulations'. This situation leads us to the statement by the Appellate Body in *Brazil – Retreaded Tyres* in the sense that the absence of a relationship between the measures and the objectives indicates that the measures discriminate in an 'arbitrary or unjustifiable' way. For example, jurisdictions in different situations as regards Argentina's access to information are classified in the same category; and jurisdictions in a similar situation as regards Argentina's access to information are placed in different categories.[175]

[168] *Ibid.* WTO, *Argentina – Measures Relating to Trade in Goods and Services – Report of the Panel* (*Argentina – Financial Services*), 9 May 2016, WT/DS453/R, para. 7.586, paras 7.595–7.596, referring to WTO, *Colombia – Indicative Prices and Restrictions on Port of Entry – Report of the Panel*, 27 April 2009, WT/D366/R, para. 7.514; and *United States – Measures Relating to Shrimp from Thailand – Report of the Panel*, 29 February 2008, WT/DS343/R, para. 7.174. The panel also refers to WTO, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef – Report of the Appellate Body*, 11 December 2000, WT/DS161/AB/R & WT/DS169/AB/R, para. 157.

[169] See WTO, *Argentina – Measures Relating to Trade in Goods and Services – Report of the Appellate Body*, 9 May 2016, WT/DS453/AB/R, para. 6.203.

[170] *Ibid.*, paras 6.203–6.205.

[171] *Argentina – Financial Services*, *supra* note 168, paras 7.661, 7.558–7.660. The panel referred to the Appellate Body reports in *US – Gambling*, *supra* note 167, para. 304, and WTO, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products – Report of the Appellate Body*, 22 May 2014, WT/DS400/AB/R & WT/DS401/AB/R, paras 5.169, 5.214.

[172] *US – Gambling*, *supra* note 167, para. 292; *Argentina – Financial Services*, *supra* note 168, para. 7.586.

[173] *US – Gambling*, *supra* note 167, para. 339.

[174] *Ibid.* Anonymous, 'A Dual Track Approach to Challenging Chinese Censorship in the WTO: The (Future) Case of Google and Facebook Note', 34 *Michigan Journal of International Law* (2012) 857, at 887.

[175] *Argentina – Financial Services*, *supra* note 168, para. 7.761.

The panel concluded that the measures at issue constituted arbitrary and unjustifiable discrimination within the meaning of the chapeau.[176] Article 4.6(e)(ii) of the EVIPA is essentially identical to paragraph (c)(ii) of Article XIV of the GATS.[177] Therefore, in an arbitration brought pursuant to the EVIPA, a tribunal could use the two-tier analysis to determine the applicability of the data protection law of a respondent state.

In contrast to the GATS, investment treaties and FTAs (for example, the USMCA, the CPTPP and the China-Australia FTA) often do not provide enough guidance to tribunals as to how to scrutinize the application of the data protection law of a respondent state. The provisions of the general exceptions in the CPTPP, the USMCA and the China-Australia FTA incorporate paragraph (c)(ii) of Article XIV of the GATS.[178] However, this does not necessarily mean an investment arbitration tribunal can rely on the two-tier analysis under Article XIV to prevent a respondent state from abusing the application of its data protection law. This is because Article XIV is incorporated into only listed chapters of the FTAs such as trade in services, the temporary entry for business persons and e-commerce/digital trade.[179] The investment chapter is not on the list.[180] Moreover, although trade in services is related to investment (the third mode of trade in services is commercial presence that involves investment),[181] this does not automatically make Article XIV of the GATS applicable to investment arbitration proceedings.

Nevertheless, Rule 19 of the ICSID Arbitration Rules allows a tribunal to make the orders required for the conduct of the proceeding.[182] A tribunal is encouraged to maintain the balance of power between the investor and the respondent state regarding the application of data protection laws. In this exercise, the spirit of Article XIV of the GATS may serve as a valuable reference. For example, the tribunal may inquire whether the proposed protective measure can secure compliance with the applicable data protection law, whether the protection is necessary to secure the compliance, whether the protection can be applied in a justifiable manner that does not frustrate the other party's legitimate rights and whether there are any reasonably available alternatives to the contested protective measure that can better balance the public interest in transparency, personal information protection and fair and efficient dispute resolution. These factors can hopefully help the tribunal address the scenario in which a party relies on a local data protection law to block the opposing party's access to crucial information in arbitration.

[176] *Ibid.*

[177] EVIPA, *supra* note 18, Art. 4.6 uses 'investment' to replace 'trade in services' in GATS, *supra* note 19, Art. XIV – e.g. 'a disguised restriction on covered investment' instead of 'a disguised restriction on trade in services'.

[178] E.g. CPTPP, *supra* note 16, Art. 29.1.3; China-Australia FTA, *supra* note 17, Art. 16.2.2; USMCA, *supra* note 15, Art. 32.1.2.

[179] E.g. CPTPP, *supra* note 16, Art. 29.1.3; China-Australia FTA, *supra* note 17, Art. 16.2.2; USMCA, *supra* note 15, Art. 32.1.2.

[180] E.g. CPTPP, *supra* note 16, Art. 29.1.3; China-Australia FTA, *supra* note 17, Art. 16.2.2; USMCA, *supra* note 15, Art. 32.1.2.

[181] GATS, *supra* note 19, Art. 1.2(c).

[182] ICSID Arbitration Rules, *supra* note 71, Rule 19.

C *Legal Divisibility and the Functional Approach*

A local data protection law may be applicable even in cases where the parties have not expressly agreed to it. Suppose that, in *Tennant*, the arbitration involved data on European citizens (for example, a witness who is a European citizen). Applying *Land Hessen*, the processing of this witness' personal data likely needs to comply with the GDPR because the data processing, regardless of where it takes place, is related to the offering of dispute resolution services for a data subject in the EU.[183] If there are witnesses from other countries, the local data protection laws of those countries may have to be applied as well. Consequently, the tribunal has to consider the application of multiple data protection laws.

The tribunal has two options. The first is to adopt legal divisibility, meaning applying different data protection laws to different data subjects. This view is endorsed by the CJEU in *Google LLC*.[184] The CJEU held that there is no obligation under EU law for a search engine operator who grants a request for de-referencing made by a data subject following an injunction from a supervisory or judicial authority of an EU member state to carry out the de-referencing on all the versions of its search engine.[185] Such a de-referencing request is limited to the versions of its search engine corresponding to the member states.[186] Placing this in the arbitration context, *Google LLC* suggests that an arbitral tribunal should differentiate the applicable data protection laws according to the data subjects.

However, legal divisibility will likely bring messy conflict-of-laws issues because data protection laws in different jurisdictions may prescribe protection differently. Complying with multiple different data protection laws is also costly and complicated, if not impossible. This may significantly increase the money and time that parties spend on compliance or disputing what information should be protected and how. To avoid these issues, an alternative option that the tribunal has is to adopt the functional approach.[187] It enables the tribunal to decide which law should be applied to a dispute based on the perceived demands of justice.[188]

The protection of personal information of multiple witnesses in an investment arbitration resembles the protection of debtors in the global assignment of debts. This is because the assignment of debts often involves debtors from different jurisdictions where mandatory financial regulations vary, which is similar to the differing mandatory data protection laws for witnesses who have different domiciles. Tribunals have to

[183] GDPR, *supra* note 1, Art. 3.2(a).

[184] *Google LLC*, *supra* note 132.

[185] *Ibid.*, paras 62, 65.

[186] *Ibid.*, para. 66.

[187] The functional approach is a way to decide the applicable law. See M. Davies *et al.*, *Nygh's Conflict of Laws in Australia* (10th edn, 2020), at 365, 375.

[188] The prominent cases using the functional approach to decide the applicable law are *National Bank of Greece and Athens v. Metliss*, [1958] AC 509, 525 (asking '[w]hat does justice demand in such a case as this?'); *Adams v. National Bank of Greece and Athens*, [1961] AC 255. For comments, see R. Mortensen, R. Garnett and M. Keyes, *Private International Law in Australia* (3rd edn, 2015), at 191.

decide whether the protection of debtors should depend on the laws of their domiciles, which resembles in investment arbitration whether the protection of personal data of witnesses should vary according to the laws of their domiciles.

In *Raiffeisen Zentralbank Osterreich AG v. Five Star General Trading LLC*, the ship owners insured the *Mount I* with French insurers under a policy of marine insurance governed by English law.[189] By a deed of assignment, also governed by English law, the ship owners purported to assign to the bank all their rights. A valid notice of assignment was given to the French insurers according to English, but not French, law. Later, after the *Mount I* collided with and sank another vessel, the bank sought declarations in the UK that all money payable by the French insurers arising out of the casualty was payable to the bank. The cargo owners disagreed and argued that the dispute was essentially a proprietary issue to be resolved by the *lex situs* of the attached debt – that is, French law. The English court held that English law should be applied because 'it may well not be appropriate to adopt a rule which would make the validity of assignment depend upon consideration of the residence of each debtor and *lex situs* of each debt assigned'.[190] Although all the co-insurers were French resident companies, the Court, by applying the functional approach, held that:

> [u]nder a typical co-insurance involving insurance from different countries, the *lex situs* rule could require the separate consideration of each of a large number of different laws of the situs, with a view to determining separately, as regards each insurer's proportionate share, the validity of a purported assignment of insurance proceeds. That would undermine the general intention, evident in the present case in the leading underwriter provisions, that there should be a homogeneous treatment of insurance underwriting and claims.[191]

The functional approach invites a clear judicial admission to a policy preference for whether a foreign law should be given effect to, not only in the circumstances of the particular case before the tribunal but also in all like cases in the future.[192] Therefore, the approach should not be considered as a plea to invite the tribunal to make an ad hoc decision considering the peculiarities of that case.[193] When handling the conflicts between multiple data protection laws, the tribunal may consider the application of one data protection law that offers the highest protection or can best be reconciled with other applicable data protection laws. Complying with one data protection law rather than multiple laws is not only cost-effective but also creates certainty and predictability for dispute resolution, which is in line with the intentions of the parties, who likely do not envision the application of multiple data protection laws. Alternatively, the tribunal may consider selecting the law that best endorses generally recognized international standards for personal data protection. Further, the tribunal should consider avoiding the application of the data protection law that has parochial

[189] *Raiffeisen Zentralbank Osterreich AG v. Five Star General Trading LLC*, [2001] QB 825.

[190] *Ibid.*, para. 38.

[191] *Ibid.*

[192] *Chaplin v. Boys*, [1971] AC 356, at 392 (holding that 'a not insubstantial makeweight … is to be found in a policy preference for the adopted solution').

[193] Davies, *supra* note 187, at 377.

requirements such as unequal protection of data subjects or extensive, unreasonable localization regulations.

D *The Brussels Effect*

The Brussels Effect refers to the EU's unilateral power to regulate global markets without needing to resort to international institutions or to seek other nations' cooperation.[194] In data protection, the Brussels Effect entails that market powers such as multinational companies voluntarily extend the GDPR to govern their global operations.[195] The Brussels Effect in relation to data protection might also occur in investment arbitration for three reasons. First, the GDPR's protection of European data subjects regardless of where the data processing takes place makes its jurisdiction both extraterritorial and highly inelastic.[196] Arbitral participants are also incentivized to comply with the GDPR due to its heavy sanctions and vigorous enforcement.[197] Second, adjudicators often tend to apply the law with which they are most familiar.[198] In investment arbitration, many arbitrators and lawyers are based in the EU and are data 'controllers' or 'processors' under the GDPR, and so are more familiar with the GDPR than the data protection laws of other jurisdictions. Last but not least, many countries have adopted data protection laws that resemble the GDPR, which means that, if the GDPR is complied with, other data protection laws will likely not be breached.[199]

The Brussels Effect produces both benefits and challenges. The benefits include predictability and certainty in relation to the applicable data protection law. Moreover, complying with the GDPR may turn out to be more cost-effective than complying with multiple data protection laws.[200] Nevertheless, the fundamental challenge is that without the parties' consent, the tribunal needs to justify why the GDPR is applicable to arbitrations conducted under a treaty to which neither the EU nor its member states is a party. Overall, it remains to be seen whether the Brussels Effect really will take hold in investment arbitration.

[194] See generally A. Bradford, *The Brussels Effect: How the European Union Rules the World* (2020).

[195] *Ibid.*, at 132, 143, 144.

[196] *Ibid.*, at 142.

[197] Although, currently, GDPR enforcement mainly focuses on data companies, it is unwise to assume that data protection agencies of the EU member states will not enforce the GDPR in an arbitration context. Non-compliance with the GDPR may result in administrative fines of up to 20 million euro or up to 4 per cent of the company's total worldwide annual turnover of the preceding financial year, whichever is greater.

[198] E.g. in *Voth v. Manildra Flour Mills Pty Ltd*, (1990) 171 CLR 538 at 559, the High Court of Australia held that 'the courts of this country are better adapted to apply a test which focuses upon the inappropriateness of the local court of which the local judge will have both knowledge and experience than to a test which focuses upon the appropriateness or comparative appropriateness of a particular foreign tribunal of which he or she is likely to have little knowledge and no experience'.

[199] Bradford, *supra* note 194, at 148–153.

[200] *Ibid.*, at 236–240 (Bradford refutes the criticism that the Brussels Effect increases costs and deters innovation).

5 Conclusion

The global investment arbitration community needs a deep understanding on the impacts of the applicability of local data protection laws. This is because the concept of privacy varies in different jurisdictions.[201] The local data protection laws can be used for protecting human rights, shifting the power of arbitration proceedings, maintaining national security, achieving digital surveillance and so on.[202] The protection of personal data should not disrupt the settled conflict-of-laws rule in investment arbitration: the primary source for the applicable law should be parties' joint consent. The consent can include parties' choice of law, the *lex arbitri*, the treaties and the procedural rules to which an arbitration is pursuant. Beyond the consensual application, arbitral participants may invoke privileges and immunities under public international law to be exempt from compliance with mandatory local data protection laws. The tribunals should strike a balance between public interest in accessing information, personal data protection and the opposing party's interest in fair and efficient dispute resolution. In this exercise, the tribunals can hopefully draw useful references from the two-tier analysis under paragraph (c)(ii) of Article XIV of the GATS and the functional approach. States, when drafting international investment treaties, should provide equal opportunities to the application of the data protection laws of the respondent state and the investor's home state.

[201] See notes 131–134 above and the accompanying texts.
[202] *Ibid.*