Asian Journal of International Law (2023), **13**, 342–364
doi:10.1017/S2044251322000595

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Data as Assets in Foreign Direct Investment: Is China's National Data Governance Compatible with its International Investment Agreements?

Cheng BIAN

Erasmus School of Law, Erasmus University Rotterdam, the Netherlands
Email: bian@law.eur.nl

(Received 25 June 2022; revised 26 September 2022; accepted 5 October 2022;
first published online 21 November 2022)

Abstract

To foreign investors, data, either collected and processed before or after market entry in the host state, can be regarded as a part of the investment and subject to the protection of the applicable international investment agreements (IIAs). China has been developing rigorous and stringent data governance such as data localization requirements and mandatory business-to-government data sharing, and has also concluded the world's second largest IIA regime that provides sweeping investment protection. There is a risk of incompatibility between China's national data policies and its IIA obligations. Foreign investors may challenge China's national laws and practices on data governance, for alleged breaches of investor's protection obligations in Chinese IIAs, or breaches of the data residency provisions in Chinese trade and investment agreements. As a result, potential exists for such claims to be brought against China in investor-state arbitration.

Keywords: China; cross-border data transfer; data governance; data localization; international investment law; mandatory business-to-government data sharing

Foreign investors and their investments are particularly sensitive and are exposed to the host state's domestic law strictures on data governance. To protect national security, data security, cyber security, and personal privacy, national laws oftentimes prohibit or significantly restrict the absolute free flow of cross-border data, which leads to rules concerning the localization of data. To protect public interest, implement public policy, or guarantee public safety, some national laws also impose compulsory business-to-government data sharing requirements. On the other hand, with regard to cross-border data transfer, international investment laws can portray a two-fold effect. Traditional investor protection provisions, such as the prohibition of performance requirements, fair and equitable treatment, and expropriation clauses may be relevant and applicable to data-backed investment when the investor decides to challenge the host governments' specific measures or even domestic laws in general by invoking these IIA provisions. Furthermore, some more recently concluded free trade agreements (FTAs) with an investment chapter also include provisions on data residency that apply to the investment chapter; such provisions, in principle, prohibit data localization and/or laws concerning the localization of computing facilities in the host state. As a result, there is a *prima facie* conflict of interests and objectives between national law and international law: the

© The Author(s), 2022. Published by Cambridge University Press on behalf of the Asian Society of International Law. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

former aims to achieve data localization and mandatory data sharing with the host government to protect national interests and personal privacy, whereas the latter attempts to encourage and promote the free flow of data across national boundaries to the benefit of the digital economy or, at the very least, not impose an impediment to digital trade and investment.

This potential conflict and incompatibility could not be more pronounced in the case of China. China's national laws on data governance impose far-reaching mandatory business-to-government data sharing requirements, granting the Chinese government systematic access to business and private data. These data-sharing requirements cover an extensive range of sectors, are implemented by a number of laws, regulations, policies, national projects, and databases, and aim for a variety of objectives and purposes and, *inter alia*, China's e-government construction and informatization process. Foreign investors are particularly concerned about the confidentiality of their data after it has been obtained by the authorities, or if implementation would be discriminatory against foreign investors.[1] Further, China adopts data localization policies, scattered in various laws and regulations such as, *inter alia*, the *National Security Law*,[2] *Cybersecurity Law*,[3] *Data Security Law*,[4] *Personal Information Protection Law*,[5] and *Measures for Cybersecurity Review*.[6] China is considered a country that promotes data localization laws and policies and adopts broad data localization rules; namely, a general application to all types of data and across various sectors.[7] However, China has also been accused by the United States (US) of imposing heavy data localization requirements, such as the prohibition and restriction of cross-border data transfer on foreign companies that "are fundamental to any business activity", local data storage and processing requirements, and "technology localization policies by encouraging the replacement of foreign information and communications technology (ICT) products and services with domestic ones", all of which are implemented allegedly for protectionist purposes.[8]

Meanwhile, China has entered into 145 bilateral investment treaties (BITs) and 24 treaties with investment provisions (TIPs), which include Hong Kong, Macao, and Taiwan.[9] This means China has the world's second largest IIA network after Germany. Concluded since the early 1980s, Chinese BITs can be divided into different generations.[10]

[1] For a detailed discussion, see Section III.A below.

[2] 国家安全法 (National Security Law) (Promulgated by the National People's Congress (NPC) on 1 July 2015, effective on promulgation).

[3] 网络安全法 (Cybersecurity Law) (Promulgated by the NPC on 7 November 2016, effective on 1 June 2017).

[4] 数据安全法 (Data Security Law) (Promulgated by the NPC on 10 June 2021, effective on 1 September 2021).

[5] 个人信息保护法 (Personal Information Protection Law) (Promulgated by the NPC on 20 August 2021, effective on 1 November 2021).

[6] 网络安全审查办法 (Measures for Cybersecurity Review) (Promulgated by Cyberspace Administration of China *et al.* on 28 December 2021, effective on 15 February 2022).

[7] John SELBY, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?" (2017) 25(3) International Journal of Law and Information Technology 213 at 215.

[8] United States Trade Representative, "2019 Report to Congress on China's WTO Compliance" (March 2020), online: USTR <https://ustr.gov/sites/default/files/2019_Report_on_China%E2%80%99s_WTO_Compliance.pdf> at 52 and 37.

[9] United Nations Conference on Trade and Development, "Investment Policy Hub, International Investment Agreements Navigator, China", online: UNCTAD <https://investmentpolicy.unctad.org/international-investment-agreements/countries/42/china>.

[10] For example, according to Berger, Chinese BITs are categorised into four generations: the first generation from 1982 to 1991 is restrictive BITs signed with developed countries based on a European model of treaty making, the second generation is restrictive BITs signed with developing countries from 1992 to 1997, also based on a European model. The third generation marks a shift to more liberal BITs based on the European model from 1998 to 2011, and the fourth generation, signed since the late 2000s based on the North American model, emanates an incoherent rebalancing between investors' protection and host states regulatory space. See Axel BERGER, "The Political Economy of Chinese Investment Treaties" in Ka ZENG, ed., *Handbook on the International Political Economy of China* (Cheltenham: Edward Elgar, 2019), 151 at 154–9.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

Before the 2010s, Chinese IIAs typically followed a traditional European model of BIT making, which is a practice followed by European countries, led by the Netherlands and Germany, that is "simple in content and narrow in coverage, focusing on protection of foreign investment in the post-establishment stage".[11] Since the China-Canada BIT (2012), Chinese BITs have witnessed a shift towards the American style, which is "much more comprehensive and complicated, often featuring detailed provisions, broader coverage, more self-contained structure, and a higher level of enforceability".[12] As a result, since only 2% of Chinese BITs (3 out of 145) and 41% of Chinese TIPs (10 out of 24) were concluded after the China-Canada BIT (2012), the majority of Chinese IIAs still follow a European style.[13] On the one hand, Chinese IIAs, in general, define "covered investment" as "every kind of asset" of the foreign investor, which in theory does not exclude data as foreign investors' assets under the protection of the investment treaty.[14] On the other hand, the majority of Chinese IIAs based on the European model provide sweeping protection to foreign investors and their investment without much elaboration on the margin of interpretation and, *inter alia*, fair and equitable treatment (FET) and protection against unlawful expropriation, thus giving rise to claims in investor-state dispute settlement (ISDS) of breaches of the treaty when a foreign investor alleges that it has suffered actual or anticipated loss because of China's laws, policies, and measures on data governance.

This article investigates this duelling tension between national laws on data governance and international investment law, and expounds on how and to what extent this potential conflict could come into light in law and adjudication, using China as a case study. Section I distinguishes personal data from non-personal and anonymized data, and discusses whether and how non-personal and anonymized data, whether collected and processed by the foreign investor before or after the market entry in the host state, can be considered as digital assets belonging to foreign investors and regarded as an integral part of their investment. Focusing on a general landscape of international investment law, Section II presents how data can be read into the definition of investment in IIAs as a covered investment and thus be qualified under treaty protection, and how investors may, albeit only in theory and not yet found in any existing ISDS cases, seek protection under various treaty provisions in this regard. Section III turns to the specific case of China and discusses its national laws on data governance, elaborating in particular on its mandatory business-to-government data sharing laws and its data localization schemes, and identifies their overall ambiguous and inclusive nature. Section IV demonstrates the potential discord between China's commitment made in IIAs to protect foreign investors and their investments and China's rigorous yet vague national laws on data governance. When it comes to data, Section V concludes that China's IIA regime appears to be in a dichotomy that creates some facilitation and remedy for foreign investors on the one hand, but imposes an excessive burden on China as the host state on the other.

I. Data as Digital Assets of Foreign Investors

Data property rights in the legal realm are still a tentative concept, although much debate exists on the necessity and feasibility of the introduction of such a concept.[15] Property rights and data involve the question of "who owns processed, value-added data for

[11] Manjiao CHI, "From Europeanization Toward Americanization: The Shift of China's Dichotomic Investment Treaty-Making Strategy" (2017) 23(2) Canadian Foreign Policy Journal 158 at 164.

[12] *Ibid.*

[13] UNCTAD, *supra* note 9.

[14] For a detailed discussion, see Section IV.A below.

[15] P. Bernt HUGENHOLTZ, "Against "Data Property" in Hanns ULLRICH, Peter DRAHOS and Gustavo GHIDINI, eds., *Kritika: Essays on Intellectual Property*, Vol. 3 (Cheltenham: Edward Elgar, 2018), 48.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

commercial transaction purposes".[16] As a premise, it is first and foremost imperative to distinguish personal data from non-personal and anonymized data. Personal data, which includes any data that identifies a person, is protected and regulated by data privacy laws such as the European Union's (EU) General Data Protection Regulation (GDPR), and cannot be the subject of property protection (other than that of the personal data owner itself).[17] It is non-personal and anonymized data that may involve the attribution of property rights.

Different jurisdictions are developing various concepts and approaches in formulating data property rights. In the EU, the Commission published a Working Document in 2017, which proposed among other approaches, a "data producer's right for non-personal or anonymized data", "with the objective of enhancing the tradability of non-personal or anonymized machine-generated data as an economic good".[18] China has not yet developed any *de jure* rules on data property rights but appears to have adopted a *de facto* approach in recognizing data controllers and processors' property rights, such as the establishment of the Shanghai Data Exchange in 2021, which trades processed data products as a commodity.[19] From a normative perspective, data may become a property right of a company that collects, extracts, processes, exploits, or accesses massive data that was derived from natural persons as raw data, which is also known as the commodification process of data.[20] Some also propose a dualist model of data governance that recognizes both the privacy rights of data subjects and the property rights enjoyed by data dealers and controllers.[21] According to this proposed model, when data is not processed but is raw/without any added value, the data subjects should have the right to their own personal data; once data is collected and processed, it is the data processors and controllers who enjoy the property rights of processed data, which have now been generalized without information allowing for identification and have added commercial value.[22] The status quo of protection of the rights of data controllers and processors is that although no property rights over data are established, it is recognized that "there are pertinent adjunct types of property protection or that property protection can be simulated to a degree"; such a right can be protected within the current legal framework such as through database protection, copyright, trade secrets protection, contract, and competition laws.[23] It remains to be seen in the future if data property rights will be recognized and protected as a right *in rem*, or if it will otherwise be read into the existing legal framework of property rights protection.

Data as assets of the foreign investor can be generated either in the pre-establishment or the post-establishment phase. In the first scenario, data could be generated before an investment is made in the host state. For example, a multinational pharmaceutical company, which is the holder of clinical data collected from the home state or other

[16] Xiaolan YU and Yun ZHAO, "Dualism in Data Protection: Balancing the Right to Personal Data and the Data Property Right" (2019) 35 Computer Law & Security Review 1 at 2.

[17] Ivan STEPANOV, "Introducing a Property Right over Data in the EU: The Data Producer's Right – An Evaluation" (2020) 34(1) International Review of Law, Computers & Technology 65 at 70.

[18] European Commission, "Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy – Accompanying the Document Communication Building a European Data Economy" (10 January 2017), online: EC <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0002> at 33.

[19] SHI Jing, "Shanghai Launches Data Exchange" *China Daily* (26 November 2021), online: The State Council of the People's Republic of China <http://english.www.gov.cn/news/topnews/202111/26/content_WS61a04d80c6d0df57f98e5977.html>.

[20] Jannice KÄLL, "The Materiality of Data as Property" (2020) 61 Harvard International Law Journal Frontiers 1 at 3.

[21] Yu and Zhao, *supra* note 16.

[22] *Ibid.*, at 6.

[23] Stepanov, *supra* note 17 at 73.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

jurisdictions, may be required to submit these clinical data to the drug regulatory authority of the host state in order to gain market access approval. One comment notes that "costs related to conducting clinical trials" prior to an investment is made for a purpose of market access approval at the host state "can be seen as related expenditures (akin to the notion of the "pre-investment" that enables business operations in a host state)".[24] Therefore, "clinical dossiers would form a part of a foreign investment, as they would enable an enterprise to obtain marketing authorization and perform business operations in a host state".[25]

In the second scenario, data could be collected and generated after the establishment of an investment. For example, investment could be made in a digital firm (either as a greenfield project or as a takeover) that "provide[s] purely digital and mixed goods and services, such as electronic payment support, cloud storage, e-commerce platforms, content and media, search engines, and social networks".[26] Additionally, for investment other than in digital companies, the digitization of traditional industries generates immense data in their business operations. In both types of companies the ownership of data is decisive in determining whether data originated post-establishment form an integral part of investment (akin to profits from the investment), which ultimately depends on the domestic law of the host state.

In sum, matters regarding substantive rights and ownership of data (if an entitlement of property rights in data is recognized and, if so, who will be entitled to what kind of property rights) are likely to be addressed differently from jurisdiction to jurisdiction, and would evolve over time.[27] If, according to the laws of the host state, data could be protected as, or similar to, a property right, and data ownership is attributed wholly or in part to the investor as the business operator, then such data should qualify as a part of the foreign investment. At the very least, non-personal and anonymized data generated either in the pre-establishment or in the post-establishment phase of an investment could be regarded as digital assets of the foreign investors, analogous to pre-investment or profits of investment.

II. IIA Provisions with Relevance to Data-based Foreign Investment

If data and other digital assets alike can be regarded as a part of an investment, further discussions are warranted regarding whether and how investor's data can be protected under the framework of IIAs and whether investors can resort to ISDS when such investment suffers from financial loss due to the host state's data governance. This Section first expounds on whether, and if yes, how, data can become a covered investment under the protection of an applicable IIA from the perspective of both the definition of an "investment" in IIAs and investment arbitration jurisprudence. This Section then delves into specific and substantive treaty obligations that may potentially be invoked by investors as a treaty breach against host states when the investor has to comply with the host state's data laws, policies, and practices, such as mandatory data sharing and data localization requirements. In particular, FET, expropriation, and data residency provisions are discussed in great detail.

[24] Daria KIM, "Protecting Trade Secrets under International Investment Law: What Secrets Investors Should Not Tell States" (2016) 15 John Marshall Review of Intellectual Property Law 999 at 1007.

[25] *Ibid.*, at 1011.

[26] Julien CHAISSE and Cristen BAUER, "Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration" (2019) 21(3) Vanderbilt Journal of Entertainment & Technology Law 549 at 556.

[27] Kim, *supra* note 24 at 1010.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

A. Data as a Subject Matter

1. Definition of investment in IIAs

Whether data can be regarded as a part of covered investment under an IIA is a question of significant importance and ramifications, because it will subsequently determine whether data can be protected under that IIA and whether an investor can resort to investor-state arbitration (ISA) if there is an alleged breach of treaty obligation. IIAs, first and foremost, define the coverage of the subject matter under the protection of the treaty; namely, the definition of "covered investment". If an investment is defined as covering intellectual property (IP) or undisclosed information such as commercial secrets, then data as a part of the investment could in principle be considered under the protection of the treaty. One empirical study found that out of 657 BITs in the Asia-Pacific region under review, 650 include IP as qualified investment,[28] such as the Japan-Myanmar BIT (2013).[29] Data packages, data collections, and databases would appear to fit in the category of undisclosed information or commercial secrets, and data-based technology, such as algorithms, source codes, computer software, or digital currency, could be protected under copyright or know-how and, therefore, be subject to the protection of the treaty at issue.

Another strand of BITs and TIPs, led by US treaty practice, defines a covered investment as "every kind of asset"; for example, the US Model BIT (2012).[30] Almost identical stipulations are found in the EU-Canada Comprehensive Economic and Trade Agreement (CETA)[31] and the German Model BIT (2008),[32] among others.[33] Apparently, the "asset-based" definition of investment has left ample room for interpretation in arbitration practice, and different tribunals have taken divergent approaches in defining it. Some tribunals have adopted a broad and straightforward approach that includes "any asset" of some economic value as covered investments, while some scholars argue that a more cautious and narrow interpretation should be considered in order not to

[28] Susan F. STONE, Soo Hyun KIM and Lars ENGEN, "Science, Technology, and Innovation in International Investment Agreements in the Asia-Pacific Region", United Nations Economic and Social Commission for Asia and the Pacific, Trade Investment and Innovation, Working Paper No. 3/2017, 30 October 2017 at 14.

[29] *Agreement Between the Government of Japan and the Government of the Republic of the Union of Myanmar for the Liberalisation, Promotion, and Protection of Investment*, 15 December 2013 (entered into force 7 August 2014) [*Japan-Myanmar BIT (2013)*]. Article 1 (a) of the Japan-Myanmar BIT (2013) defines "investment" as including "(vi) intellectual property rights, including copyrights and related rights, patent rights and rights relating to utility models, trademarks, industrial designs, layout designs of integrated circuits, new varieties of plants, trade names, indications of source or geographical indications and undisclosed information".

[30] United States Trade Representative, "2012 U.S. Model Bilateral Investment Treaty" (April 2012) online: USTR <https://ustr.gov/sites/default/files/BIT%20text%20for%20ACIEP%20Meeting.pdf> [*US Model BIT (2012)*], section A, art. 1. The US Model BIT (2012) defines covered investment as "every asset that an investor owns or controls, directly or indirectly, that has the characteristics of an investment, including such characteristics as the commitment of capital or other resources, the expectation of gain or profit, or the assumption of risk."

[31] *Canada-European Union Comprehensive Economic and Trade Agreement,* 30 October 2016 (entered into force provisionally 21 September 2017) [*CETA*]. Article 8.1 of CETA defines "investment" as "every kind of asset that an investor owns or controls, directly or indirectly, that has the characteristics of an investment, which includes a certain duration and other characteristics such as the commitment of capital or other resources, the expectation of gain or profit, or the assumption of risk".

[32] German Federal Ministry for Economics and Technology, "German Model Treaty – 2008" online: UNCTAD <https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/2865/download> [*German Model Treaty (2008)*]. Article 1.1 of the German Model Treaty (2008) defines "investment" as to "comprise every kind of asset which is directly or indirectly invested by investors of one Contracting State in the territory of the other Contracting State."

[33] Chaisse and Bauer, *supra* note 26 at 557.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

overburden the contracting states with obligations of investment protection.[34] Until now, tribunals have not yet had the opportunity to contend with whether data can be classified as an investment under an IIA. From an economic standpoint, with the advent of the information age, there is no doubt that data is an important, if not the most important, economic asset and production resource owned and controlled by businesses. However, it remains to be seen if arbitral tribunals would count data as an asset under the legal definition of a covered investment in IIAs should such cases arise in the future.

With that being said, due to the fact that data ownership – i.e. who owns what kind of data and what rights does data ownership warrant – is still a developing concept and the legal framework is still in formulation; it is not yet completely clear if investors can claim data that is generated, collected, stored, processed, controlled, or accessed by them as invested assets under the protection of IIAs. The emergence and proliferation of data-based businesses calls for the modernization of international investment lawmaking in general, as well as the adaptation of the interpretation of IIAs in ways that could accommodate the ever-changing digital economy context.

2. Definition of investment in ISA

Even when the BIT at issue neither explicitly includes IP nor "every asset" as covered investment, IP "can be defined as an investment through treaty language allowing for an accommodating interpretation".[35] For example, according to Sornarajah, foreign investment "involves the transfer of tangible or intangible assets from one country into another for the purpose of their use in that country to generate wealth under the total or partial control of the owner of the assets".[36] Some arbitral tribunals have also interpreted "investment" in such a way as to include intangible assets as long as a four-part test was met, which was first formulated in the case of *Salini et al. v. Morocco* and acknowledged and cited in many subsequent cases of a similar nature.[37] This four-part test, also known as the *Salini* test, defines an investment as "(1) a contribution of money or assets; (2) a certain duration; (3) an element of risk; and (4) a contribution to the economic development of the host state."[38] Other tribunals have either followed the *Salini* test in whole or in part in their jurisprudence, or added more factors for consideration to the original test.[39] For example, in the case of *Philip Morris v. Uruguay*, the tribunal sided with the investor in arguing that trademarks constituted an investment, even if trademarks only fulfilled the first three elements of the *Salini* test but "essentially exclude the notion of economic development as a constitutive element of the concept of investment".[40] With regard to digital assets, it "support[s] an arguable path for including digital assets as investments under BITs".[41] For example, to establish a tech company in the host state, the foreign investor usually has to invest a substantial amount of money and resources in the market access phase over a certain period of time, which also entails a significant degree of business and regulatory risk in order to see any economic benefit and return in profit, thus satisfying at least a substantial part of the *Salini* test.

[34] *Ibid.*, at 559.

[35] Ivan STEPANOV, "Economic Development Dimension of Intellectual Property as Investment in International Investment Law" (2020) 23(5) Journal of World Intellectual Property 736 at 741.

[36] M. SORNARAJAH, *The International Law on Foreign Investment*, 4th ed. (New York: Cambridge University Press, 2017) at 14.

[37] Alex GRABOWSKI, "The Definition of Investment under the ICSID Convention: A Defense of Salini" (2014) 15 (1) Chicago Journal of International Law 287 at 290 and 296. Stepanov, *supra* note 35 at 742–4.

[38] *Ibid.*

[39] Stepanov, *supra* note 35 at 743.

[40] *Ibid.*, at 745.

[41] Chaisse and Bauer, *supra* note 26 at 563.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

B. Substantive Standards of Protection

1. Fair and equitable treatment

Almost every known ISA has made a claim on breach of FET.[42] When claims of expropriation fail, investors tend to resort to FET for protection.[43] The FET is regarded as an elusive, controversial, and obscure provision whose meaning lacks universal recognition and is subject to arbitrary interpretation.[44] Early IIAs, such as the North American Free Trade Agreement (NAFTA) and BITs concluded by European countries, often contain a succinct provision on FET that has little or no elaboration on its constituent elements.[45] A new generation of IIAs such as, *inter alia*, those negotiated by the EU after the entry into force of the Lisbon Treaty in 2009, which provides that "investment protections must be clearly defined and leave no room for interpretative ambiguity", and contains "a novel provision that enumerates in quasi-exhaustive manner" elements of FET;[46] for instance, CETA.[47] However, these new generation IIAs only account for a minute fraction of the more than 3000 IIAs concluded globally, which means the majority of IIAs still incorporate a simple FET clause, relying on the arbitral tribunals' interpretative autonomy for its scope and meaning.

Some commonly referenced elements of FET by tribunals and academia include legitimate expectations, due process, transparency, freedom from coercion and harassment, and good faith.[48] But in some of these elements there is also considerable uncertainty about its meaning and content. For instance, lacking a universally accepted definition, legitimate expectations of the investor usually posit that the municipal law of the host state, applicable treaty provisions, and undertakings made by the host state, by which an investor makes its investment decisions, altogether form the basis of legitimate expectations.[49] Tribunals have, in principle, adopted three approaches towards legitimate expectations in deciding whether there has been a breach of FET, namely: legitimate expectations can be protected even without unambiguous and express promises from the host state; legitimate expectations can possibly be protected, but the prospects for establishing an FET violation significantly decline without clear and express undertakings;

[42] According to UNCTAD, out of 1104 known ISDS cases globally from 1987 to 2020, 657 cases have clear and available data on the type of breaches of IIAs alleged by foreign investors; out of these 657 cases, 555 of them claimed a breach of FET. United Nations Conference on Trade and Development, "Investment Policy Hub, Investment Dispute Settlement Navigator, Breaches" (31 December 2021), online: UNCTAD <https://investment-policy.unctad.org/investment-dispute-settlement>.

[43] Rudolf DOLZER and Christoph SCHREUER, *Principles of International Investment Law*, 2nd ed. (New York: Oxford University Press, 2012), 132.

[44] Marc JACOB and Stephan W. SCHILL, "Fair and Equitable Treatment: Content, Practice, Method", in Marc BUNGENBERG, Jörn GRIEBEL, Stephan HOBE, and August REINISCH, eds., *International Investment Law: A Handbook* (Baden-Baden: Nomos, 2015), 700.

[45] For example, the FET provision in NAFTA reads: "Each Party shall accord to investments of investors of another Party treatment in accordance with international law, including fair and equitable treatment and full protection and security." *North American Free Trade Agreement*, 17 December 1992 (entered into force 1 January 1994) [*NAFTA*], art. 1105(1).

[46] Catharine TITI, "International Investment Law and the European Union: Towards a New Generation of International Investment Agreements" (2015) 26(3) The European Journal of International Law 639 at 654 and 656.

[47] CETA stipulates that breaches of the FET may include: denial of justice; fundamental breach of due process and transparency; manifest arbitrariness; targeted discrimination on manifestly wrongful grounds; abusive treatment of investors; and others. CETA, *supra* note 31 at art. 8.10.2.

[48] Rudolf DOLZER, "Fair and Equitable Treatment: Today's Contours" (2013) 12(1) Santa Clara Journal of International Law 7. Christoph SCHREURER, "Fair and Equitable Treatment in Arbitral Practice" (2005) 6(3) Journal of World Investment & Trade 357 at 373–4; Dolzer and Schreuer, *supra* note 43 at 145–52.

[49] Dolzer and Schreuer, *supra* note 43 at 145–9.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

and legitimate expectations must require "clear and express assurances" from the host state.[50]

In many jurisdictions, governments have the authority to require private businesses to share their massive data collected from online services and smart machines for certain purposes, such as anti-terrorism. The existence of mandatory business-to-government data sharing rules and practices have been found in at least thirteen countries,[51] and more jurisdictions are in the process of formulating such rules at present or are planning to do so. For example, there are, at the moment, no mandatory business-to-government data sharing rules at the EU level, although a High-Level Expert Group on Business-to-Government Data Sharing was established in 2020, which suggests "the Commission explore the creation of an EU regulatory framework to enable and facilitate B2G (Business-to-government) data sharing for public-interest purposes".[52] These business-to-government data sharing laws, initiatives, proposals, and practices are, in general, stipulated to cover essentially unlimited purposes for which shared data are used, which involve a significant amount of government discretion, are arbitrary in enforcement, lack transparency, and lack accountability in cases of breach of privacy, constitutional rights, or human rights.[53] As a result, national laws and policies, as well as practices pertinent to mandatory data sharing, may be challenged by foreign investors as a breach of various elements constituting the FET in the IIA if they are characterized by a lack of transparency, arbitrariness, a lack of due process in enforcement (such as a lack of administrative or judicial redress), a lack of legal certainty (such as when investors do not fully comprehend in advance how much data they control needs to be shared with the authorities of the host state), or simply negatively affect investors' legitimate expectations.

In addition to mandatory data sharing, other national legislation pertaining to data, such as cybersecurity laws, privacy protection laws, administrative and licensing processes for digital service providers, data localization requirements, and internet censorship or content restrictions, may also result in a claim of FET if they manifest as hasty modification, inconsistent, unreasonable, lacking due process, or lacking local judicial remedies.[54] If data localization requirements or the restrictions on cross-border data transfer of a host state are intended to benefit domestic companies at the expense of foreign companies – for instance, to increase the data storage and processing costs of foreign businesses which puts domestic competitors at an advantage – then foreign investors may also claim that these domestic data regulations are discriminatory towards foreign businesses and thus in violation of the FET.[55]

[50] Arwel DAVIES, "Investment Treaty Interpretation, Fair and Equitable Treatment and Legitimate Expectations" (2018) 15(3) Manchester Journal of International Economic Law 314 at 319–27.

[51] Fred H. CATE and James X. DEMPSEY, eds., *Bulk Collection: Systematic Government Access to Private-Sector Data* (New York: Oxford University Press, 2017).

[52] European Commission, "Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest: Final Report Prepared by the High-Level Expert Group on Business-to-Government Data Sharing" (15 February 2021) online: Publications Office of the EU <https://op.europa.eu/en/publication-detail/-/publication/d96edc29-70fd-11eb-9ac9-01aa75ed71a1#> at 41.

[53] Ira S. RUBENSTEIN, Gregory T. NOJEIM and Ronald D. LEE, "Systematic Government Access to Private-Sector Data: A Comparative Analysis" in Fred H. CATE and James X. DEMPSEY, eds., *Bulk Collection: Systematic Government Access to Private-Sector Data* (New York: Oxford University Press, 2017), 5.

[54] Chaisse and Bauer, *supra* note 26 at 571–6.

[55] Sheng ZHANG, "Protection of Cross-Border Data Flows Under International Investment Law: Scope and Boundaries" in Julien CHAISSE, Leïla CHOUKROUNE, and Sufian JUSOH, eds., *Handbook of International Investment Law and Policy* (New York: Springer, 2021), 209 at 221–2.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

2. Expropriation

For direct expropriation, there must be a deprivation of the title of investors' property rights. The case of indirect expropriation, however, might be less certain and more complex to determine. Indirect expropriation in itself is a murky concept that lacks an unequivocal definition. Arbitral tribunals have had to develop various standards to determine indirect expropriation, which vary greatly in rationale and outcome.[56] Some tribunals adopt the sole effects doctrine in determining indirect expropriation, whereby the tribunal will seek existence of a "substantial deprivation" of the investment,[57] including "the value, use, or enjoyment of the claimant's investment".[58] Other tribunals adopt the police powers doctrine, which considers the "purpose, context and nature" of the state measure relevant to indirect expropriation.[59] Within a broad definition of the police powers doctrine, state measures that are adopted for a public purpose are non-discriminatory and *bona fide*, and are a legitimate regulatory means rather than expropriatory acts.[60] And there are tribunals that "appear increasingly disinclined to adhere to extreme versions" of either approaches, who tend to adopt a more conciliatory approach that considers both the effect and purpose of state measures, such as a proportionality test.[61] The proportionality test attempts to find a balance between the effects of state measures to foreign investment and the objective of such measures. Similar to FET, tribunals have predominantly considered the protection of investors "legitimate expectations" in claims of indirect expropriation.[62]

Some argue that, under the standard of "substantial deprivation", data localization requirements of the host states are unlikely to amount to expropriation as they merely raise more compliance costs for foreign businesses rather than "a destruction of their ability to continue in business".[63] In the same vein, with regard to the data sharing laws and practices of a host state, in order for an investor to challenge them as indirect expropriation there are at least two significant obstacles. First, the investor will have to demonstrate that data sharing with the government of the host state would indeed lead to a substantial deprivation of the investors' property rights, and not merely an adverse effect on the economic value of an investment. This aspect can be difficult to prove, depending on how the government treats the shared data; for example, if the government keeps the data obtained confidential or whether there is an ensuing action to publicly

[56] Peter D. ISAKOFF, "Defining the Scope of Indirect Expropriation for International Investments" (2013) 3(2) Global Business Law Review 189 at 197–200.

[57] Dolzer and Schreuer, *supra* note 43 at 104.

[58] Several tribunals have applied this standard to determine "substantial deprivation", *inter alia*, *Philip Morris Brands Sàrl, Philip Morris Products S.A. and Abal Hermanos S.A. v. Oriental Republic of Uruguay*, ICSID Case No. ARB/10/7 Award (8 July 2016) at para. 192, citing from Prabhash RANJAN, "Police Powers, Indirect Expropriation in International Investment Law, and Article 31(3)(c) of the VCLT: A Critique of Philip Morris v. Uruguay" (2019) 9 Asian Journal of International Law 98 at 106–7.

[59] Ben MOSTAFA, "The Sole Effects Doctrine, Police Powers and Indirect Expropriation under International Law" (2008) 15 Australian International Law Journal 267.

[60] Noam ZAMIR, "The Police Powers Doctrine in International Investment Law" (2017) 14(3) Manchester Journal of International Economic Law 318 at 327.

[61] L. Yves FORTIER and Stephen L. DRYMER, "Indirect Expropriation in the Law of International Investment:

> I Know It When I See It, or *Caveat Investor*" (2004) 19(2) ICSID Review 293 at 326; Caroline HENCKELS, "Indirect Expropriation and the Right to Regulate: Revisiting Proportionality Analysis and the Standard of Review in Investor-State Arbitration" (2012) 15(1) Journal of International Economic Law 223.

[62] Maryam MALAKOTIPOUR, "The Chilling Effect of Indirect Expropriation Clauses on Host States' Public Policies: A Call for a Legislative Response" (2020) 22(2) International Community Law Review 235 at 243.

[63] Andrew D. MITCHELL and Jarrod HEPBURN, "Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer" (2017) 19 Yale Journal of Law and Technology 182 at 222.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

disclose the data or enable a third party to access the same. Second, since the data sharing measures are pursuing *prima facie* a public purpose, such as anti-terrorism, public security, or public health, the host state may use its right to regulate as a defence to counteract an investor's attempt of claims of regulatory/creeping expropriation. Of course, this does not mean that the right to regulate is a limitless power for the host state to justify any of its regulatory measures. The police powers doctrine, either recognized as customary international law or a general principle of international investment law, should be utilized with some confinement to its application, such as by tackling only fundamentally serious issues of public policy and by applying a reasonable, good faith, and non-discriminatory exercise of the police power.[64]

Others argue that cyberattacks on investors' data and digital assets may amount to a claim on expropriation, although it will be rather difficult to pinpoint the origin of these cyberattacks to the host state with substantiated evidence as expropriation should be, by definition, a state act.[65]

C. Provisions on Data Residency in FTAs

Some IIAs attempt to address cross-border data transfer specifically. The US-South Korea FTA (2007) stipulates that "the Parties shall endeavour to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders".[66] In contrast with the best-effort clause in the US-South Korea FTA, the Transpacific Partnership Agreement (TPP), whose text has now been inherited by the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), is the first TIP that obliges the contracting states to avoid restrictions on cross-border data flows unless justified.[67] The TPP/CPTPP also creates a modelling effect in "spurring further data-focused provisions" in subsequent mega-regional agreements, such as the Singapore-Australia FTA, the Peru-Australia FTA, and the US-Mexico-Canada Agreement (USMCA).[68] Chapter 14 of the TPP/CPTPP on electronic commerce specifically addresses cross-border data flows. Article 14.1 gives definitions of the coverage of Chapter 14, which defines "a covered person" as including a covered investment, and a covered investor as defined in the investment chapter. Article 14.11 requires the parties to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person", unless the domestic measures adopted or maintained are inconsistent with this obligation to achieve a legitimate public policy objective. Article 14.13, the so-called "data localization clause",[69] prohibits contracting states from requiring "a covered person to use or locate computing facilities" in a contracting state as a condition for conducting business in that state, unless domestic measures are adopted or maintained that are inconsistent with this obligation to achieve a legitimate public policy objective. The "public policy" exception needs to satisfy a

[64] Catharine TITI, "Police Powers Doctrine and International Investment Law", in Andrea GATTINI, Attila TANZI, and Filippo FONTANELLI, eds., *General Principles of Law and International Investment Arbitration* (Leiden: Brill, 2018), 323.

[65] Chaisse and Bauer, *supra* note 26 at 585–7.

[66] *United States-Korea Free Trade Agreement*, 30 June 2007 (entered into force 15 March 2012), art. 15.8.

[67] Neha MISHRA, "The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?" (2017) 20(1) Journal of International Economic Law 31.

[68] Lizzie KNIGHT and Tania VOON, "The Evolution of National Security at the Interface Between Domestic and International Investment Law and Policy: The Role of China" (2020) 21 Journal of World Investment & Trade 104 at 137–8.

[69] Shin-Yi PENG and Han-Wei LIU, "The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?" (2017) 51(2) Journal of World Trade 183 at 184.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

necessity test to qualify as "legitimate".[70] The term "public policy" is not defined in TPP/CPTPP, thus giving rise to ambiguity and a disparate interpretation from different contracting State Parties with different values and policies.[71]

While the objective of the TPP's drafters was to "reduce protectionism arising from data residency requirements", these obligations on contracting states may not go very far because the ambiguous "legitimate public policy" exception to these obligations may be invoked to defend national measures on data residency, which "will have strong arguments".[72] Further, foreign investors are only allowed to bring a claim of breach under Chapter 9, the investment chapter, but not Chapter 14 of TPP/CPTPP to ISA. Nonetheless, these data provisions in the TPP/CPTPP have already become a negotiating template for subsequent agreements.[73]

D. Insights

It has become clear now, at least from a theoretical standpoint, that investors face few obstacles to claim that data in their possession qualifies as an integral part of their investment and thus should be protected by IIAs. On that note, investors are in principle entitled to resort to ISA and bring claims against host states for a breach of FET, expropriation, and data residency provisions, if so provided in the treaty. Such claims can be based on investors' actual or even anticipated financial losses that result from the host states' data laws, policies, and acts, including, most significantly, mandatory data sharing with the government and data localization requirements, as well as cybersecurity laws, privacy protection laws, administrative and licensing processes in the digital service sector, internet censorship, and content restrictions, among others. Nevertheless, these claims may be difficult to establish before a tribunal, because the evidentiary burden will be quite high on the investors' side, whereby the investor will very likely be asked to demonstrate the existence of a "substantial deprivation" of its assets and direct causation between the losses suffered and the impugned state's acts.

III. Chinese Domestic Laws on Data Governance

A. Mandatory Business-to-Government Data-Sharing

The Chinese law grants the government systematic access to private data. As explained by Wang:

> In accordance with facilitating Chinese e-government construction, many laws made for the purpose of state security, public security, censorship, and taxation have granted the Chinese government extensive power of access to private-sector data generated in such businesses as information, finance, trade, travel, entertainment, and so on, operated in China.[74]

[70] The necessity test requires that the domestic measure in question on data residency: "(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective." *Trans-Pacific Partnership*, 5 October 2015, arts. 14.11.3 and 14.13.3.

[71] Mitchell and Hepburn, *supra* note 63 at 209.

[72] Peng and Liu, *supra* note 69 at 183 and 202.

[73] Zhang, *supra* note 55 at 215.

[74] Zhizheng WANG, "Systematic Government Access to Private-Sector Data in China", in Fred H. CATE and James X. DEMPSEY, eds., *Bulk Collection: Systematic Government Access to Private-Sector Data* (New York: Oxford University Press, 2017), 241 at 241.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

First, the Constitution provides that "to meet the needs of state security or of investigation into criminal offences, public security or prosecution authorities are permitted to censor correspondence in accordance with procedures prescribed by law".[75] This provision in the Constitution has been criticised for lacking explicit procedural rules or for not being known to the public, and becomes a primary source of legal ground for lower hierarchical laws and regulations to grant the government access to private data.[76] As a result, laws requiring, or explicitly authorizing, governmental access to data generated in the private sectors, such as the *State Security Law* and *Criminal Procedure Law*, allow the government to enjoy "an extensive and unrestricted power of investigation and censorship of communications whenever state security or public security is involved".[77]

Further, to build the ambitious e-government initiative and informatization process, based on a framework set forth in the *National Informatization Leading Group Guiding Opinions concerning Our Country's E-Government Construction*,[78] which is regarded by some as a tool to authorise government access to private sector data, "[I]n the name of e-government designed to reinforce its surveillance capabilities", a number of national projects and databases were established, such as the 12 Golden Projects,[79] which involve "systematic data digitalization and data collection of almost every aspect of a person's life".[80] Examples of laws and regulations enforcing the e-government process include, for instance, the *Accounting Law*, tax-related laws, and a number of computer, data, internet, and telecommunication laws that grant various government departments the power to access and censor content in the name of protecting information security.[81] All these laws and regulations are deemed to be vague in both scope and application, giving the authorities flexibility and discretion to demand data access and mandatory data retention.[82] As a result, the private sector is compelled to comply with these projects and databases for the construction of the e-government relating to security, public safety, public health, accounting, finance, taxation, insurance, and so on.

Moreover, there are laws that require broad reporting obligations of personal data to the government from the private sector. These include anti-money laundering laws and regulations require financial and non-financial institutions to report suspicious transactions to China's Anti-Money Laundering Monitoring Analysis Centre. However, many private sectors report large amounts of ordinary transactions to the Centre "in fear of missed reports of suspicious transactions" but only a few actually provide data on money laundering activities.[83] Other laws in this regard include measures for the control of security in the hospitality sector, which mandate hotels to upload guest information to government databases, mandatory sharing of air transport itineraries of

[75] 中华人民共和国宪法 (Constitutional Law of China) (Promulgated by the NPC on 11 March 2018, effective on promulgation), art. 40.

[76] Wang, *supra* note 74 at 244–5. Zhizheng WANG, "Systematic Government Access to Private-Sector Data in China" (2012) 2(4) International Data Privacy Law 220.

[77] Wang, *supra* note 74 at 244.

[78] 国家信息化领导小组关于我国电子政务建设指导意见 (National Informatization Leading Group Guiding Opinions concerning Our Country's E-Government Construction) (Issued by the General Office of the CPC and General Office of the State Council on 5 August 2002, effective on promulgation).

[79] In Chinese: 十二金工程. This includes Golden Macro Economy, Golden Tax, Golden Customs, Golden Finance, Golden Cards, Golden Auditing, Golden Insurance, Golden Agriculture, Golden Bridge, Golden Quality, Golden Travel, and Golden Medical.

[80] Wang, *supra* note 74 at 247–8.

[81] For a detailed discussion of these laws, see Wang, *supra* note 74 at 249–55.

[82] *Ibid.*, at 248.

[83] *Ibid.*, at 255–6.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

passengers, and mandatory sharing of data of audiences and staff collected at public entertainment venues.[84]

Last but not least, private businesses are also required to share their commercial and operational data with central and local government pursuant to China's industrial policy. For example, under the *Provisions on the Administration of Market Entry of New Energy Vehicles Manufacturers and Products* – which was promulgated in 2017, and recently revised in the 2020 mandate – all new energy vehicle (NEV) manufacturers, whether domestic or foreign, must establish data platforms that monitor the operation and safety of every car sold, and share these data platforms with both national and local regulators as a precondition for market entry.[85] The provisions further require NEV producers to collect detailed technical and personal information of each car, such as driving route history, repair and maintenance, battery use, and technical problems, all of which should be accessible by the provincial-level of government upon request.[86] These wide-ranging requirements are deemed by foreign-invested NEV manufacturers as a potential erosion of their commercial secrets and the privacy of drivers.[87] Another concern from foreign NEV producers is that, considering "the long tradition of non-transparency in Chinese bureaucracy", it is not clear how data obtained by the government will be put to use; for example, if these data will be provided to other governmental institutions or other private domestic competitors for their technological and commercial advancement, thus discriminatorily creating a competitive disadvantage to foreign investors.[88]

B. Data Localization

China's data localization regime follows a principled rule of "local storage, outbound assessment", pursuant to the *Cybersecurity Law*.[89] The *Cybersecurity Law* mandates that personal data and important data must be intercepted within the Chinese border; if these data are indeed necessary for business purposes to be transferred outside China, a security assessment must be conducted.[90] These data localization rules in the *Cybersecurity Law* were criticized by foreign stakeholders in particular for being protectionist, too stringent, overly broad, ambiguous, and potentially expansive in enforcement (extending to all data, not just personal and important data).[91] At the time of drafting the *Cybersecurity Law*, opposition from various foreign stakeholders was vehemently expressed, including a formal defence document against it submitted by the US to the World Trade Organization (WTO),[92] but this had little effect on the content of the law promulgated thereafter.

The *Personal Information Protection Law* promulgated in August 2021, stipulates that personal data collected and generated within the territory of China should in principle be stored domestically.[93] When an information processor has to provide personal data

[84] *Ibid.*, at 256–7.

[85] 新能源汽车生产企业及产品准入管理规定 (Provisions on the Administration of Market Entry of New Energy Vehicles Manufacturers and Products) (Promulgated by the Ministry of Industry and Information Technology on 1 June 2017, revised on 24 July 2020, effective on 1 September 2020), art. 17.

[86] *Ibid.*, at arts. 18 and 22.

[87] Bertin MARTENS and Bo ZHAO, "Data Access and Regime Competition: A Case Study of Car Data Sharing in China" (2021) 8(2) Big Data & Society 1 at 5.

[88] *Ibid.*, at 6.

[89] Jinhe LIU, "China's Data Localization" (2020) 13(1) Chinese Journal of Communication 84 at 84.

[90] Cybersecurity Law, *supra* note 3 at art. 37.

[91] Liu, *supra* note 89 at 88.

[92] World Trade Organisation, "Cybersecurity Measures of China and Viet Nam – Requested by Japan and the United States (Report of the Meeting Held on 6 October 2017)" (6 November 2017), online: WTO <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/M133.pdf&Open=True>.

[93] Personal Information Protection Law, *supra* note 5 at art. 40.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

outside China a number of conditions must be satisfied. Under any circumstance, the data processor must acquire separate consent from individuals.[94] In addition to individual consent, the data processor must also acquire approval from a security assessment undertaken by the Cyberspace Administration of China, or obtain a Certificate of Personal Information Protection by a specialized agency recognized by the Cyberspace Administration of China, or enter a contract with the overseas data recipient, which is modelled on a standard contract drafted by the Cyberspace Administration of China.[95] Unless approved by the relevant Chinese authorities, data processors are prohibited from providing personal information stored in China to foreign judicial or law enforcement authorities.[96]

Besides personal data, "important data" is also subject to data localization requirements. An operator of critical information infrastructure, which is loosely defined in the *Cybersecurity Law* as "infrastructure that might seriously endanger national security, people's livelihood, or public interest if damaged",[97] must store in China personal information and important data (a critical notion that lacks a statutory definition) that are generated and collected in China. The *Data Security Law* further imposes a number of obligations and requirements for the protection of important data beyond data localization requirements but still falls short of defining the notion of important data. The *Data Security Law* also introduces a data security review system to all data processing activities in China that may affect national security,[98] which is substantiated by the *Measures for Cybersecurity Review*. According to the Measures, a cybersecurity review shall focus on the assessment of "risks of core data, important data, or massive personal information being illegally transferred" outside China, among other risks, yet still leaves notions such as "core data" and "important data" undefined.[99]

Apart from the data laws and regulations above, there are various sectoral regulations that subject domestic and foreign companies to data localization requirements. For instance, the *Measures on the Automotive Data Security Management* requires businesses in the sector to store automotive personal data and important data in China.[100] Consequently, under China's rigorous data governance and regulations, data – including personal data and important data – should in principle be stored locally and can only be transferred overseas if it is necessary for the business operation, which will be subject to several conditions such as, for instance, an *ex-ante* security assessment. However, this process has either not yet been formulated or is formulated in a manner that is too ambiguous to comply with.

China's rigorous and broad data localization rules have already created a rippling and deterrent effect on foreign businesses. It is reported that several US companies, including Yahoo, Microsoft, LinkedIn, and Airbnb, have decided to withdraw their business and end operations in China due to mounting data compliance costs.[101] Other companies, such as Apple, have made compromises and have stored their Chinese customers' data within

[94] *Ibid.*, at art. 39.
[95] *Ibid.*, at art. 38.
[96] *Ibid.*, at art. 41.
[97] Cybersecurity Law, *supra* note 3 at art. 31.
[98] Data Security Law, *supra* note 4 at art. 24.
[99] Measures for Cybersecurity Review, *supra* note 6 at art. 10.5.
[100] 汽车数据安全管理若干规定（试行）(Measures on the Automotive Data Security Management for Trial Implementation) (Promulgated by Cyberspace Administration of China *et al.* on 16 August 2021, effective on 1 October 2021), art. 11.
[101] Kai VON CARNAP, "Beijing's Watchful Eye on all Data Flowing in and out of China" *MERICS* (8 July 2022) online: MERICS <https://merics.org/en/short-analysis/beijings-watchful-eye-all-data-flowing-and-out-china>.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

China in a state-owned Chinese data centre, which raised privacy concerns over these personal data.[102]

IV. The Incompatibility Between China's Data Governance and Chinese IIA Commitments

A. Definition of Investment

Different generations of Chinese BITs and TIPs incorporate different definitions of covered investment. Already found in the first BIT China signed with Sweden in 1982, Chinese BITs, in principle, define covered investments as "every kind of asset", including IP rights. Chinese IIAs that follow a European style, for example the China-Germany BIT (2003), usually adopt "every kind of asset" as a covered investment, together with a list of enumerated examples, including IP rights.[103] Chinese IIAs that follow an American style adopt a different approach. For example, the China-Canada BIT (2012) does not include the "every kind of asset" definition, but refers to "intellectual property rights" and "any other tangible or intangible, moveable or immovable, property and related property rights acquired or used for business purposes".[104] Chinese FTAs with an investment chapter, in principle, adopt the "every kind of asset" formula as well. For instance, the Regional Comprehensive Economic Partnership (RCEP)[105] incorporates in part the *Salini* test to define a covered investment without the requirement of economic contribution to the host state. To this end, it appears that foreign investors' data as an investment would not *prima facie* face any obstacles to be qualified as a covered investment or the need to seek protection under the Chinese IIA regime.

B. Substantive Standards of Protection

1. Fair and equitable treatment

The provisions of FET in Chinese IIAs are almost a default setting. Since the first BIT signed with Sweden in 1982, FET has been provided as part of a standard repertoire. However, as 98% of Chinese BITs follow a European style these FET provisions are rather succinct with little or no contextual elucidation in the treaty. A typical FET provision in Chinese BITs reads: "[i]nvestments of investors of each Contracting Party shall all the time be accorded fair and equitable treatment in the territory of the other Contracting

[102] Jack NICAS, Raymond ZHONG and Daisuke WAKABAYASHI, "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China" *New York Times* (17 June 2021) online: New York Times < https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html>.

[103] *Agreement Between the People's Republic of China and the Federal Republic of Germany on the Encouragement and Reciprocal Protection of Investments*, 1 December 2003 (entered into force 11 November 2005) [*China-Germany BIT (2003)*]. Article 1.1 of the China-Germany BIT (2003) provides that: "the term 'investment' means every kind of asset invested directly or indirectly by investors of one Contracting Party in the territory of the other Contracting Party, and in particular, though not exclusively, includes ... (d) intellectual property rights, in particular copyrights, patents and industrial designs, trade-marks, trade-names, technical processes, trade and business secrets, know-how and good-will".

[104] *Agreement Between the Government of Canada and the Government of the People's Republic of China for the Promotion and Reciprocal Protection of Investments*, 9 September 2012 (entered into force 1 October 2014) [*China-Canada BIT (2012)*], art. 1.1.

[105] *Regional Comprehensive Economic Partnership Agreement*, 15 November 2020 (entered into force 1 January 2022) [*RCEP (2020)*]. Article 10.1(C). of RCEP (2020) defines "investment" as "every kind of asset that an investor owns or controls, directly or indirectly, and that has the characteristics of an investment, including such characteristics as the commitment of capital or other resources, the expectation of gains or profits, or the assumption of risk".

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

Party".[106] This standard FET provision raises questions about its interpretation as some equate the minimum standard of treatment with the FET, which has been criticized by some Chinese scholars as an encroachment on China's sovereignty.[107]

Chinese IIAs that follow an American style, on the other hand, include a more elaborate FET provision. For example, the China-Canada BIT (2012) provides that "each Contracting Party shall accord to covered investments fair and equitable treatment and full protection and security, in accordance with international law", and further explains that "[t]he concepts of 'fair and equitable treatment' ... do not require treatment in addition to or beyond that which is required by the international law minimum standard of treatment of aliens as evidenced by general State practice accepted as law".[108] This means that FET under the China-Canada BIT needs to be interpreted under the principles of international law and customary international law (but not the domestic laws of the contracting states) and no minimum standard of treatment should be considered when interpreting the FET provision. The China-Mauritius FTA (2019) provides the most comprehensive provisions on FET so far, which excludes, *inter alia*, investors' expectations as the sole standard by which to determine a breach of FET.[109]

As was previously discussed, national laws, regulations, and practices pertinent to mandatory business-to-government data sharing, data localization requirements, internet censorship or content restrictions, and so on may be challenged by investors as a breach of FET. Taking China's mandatory data sharing laws and practice as an example, as was illustrated in the previous Section, China's mandatory business-to-government data sharing scheme has a broad scope of sectoral coverage that essentially leaves no exceptions. It lacks specified legal rules on how the shared data will be processed or used once obtained by the public authorities; it involves a significant amount of government discretion; it may be arbitrary in enforcement; it lacks transparency; and it lacks administrative or judicial remedies in cases of breach of private interests. As a result, foreign investors in China who are subject to these data sharing requirements may resort to ISA and claim a breach of FET according to the applicable treaty.

More specifically, as almost all Chinese IIAs negotiated before 2012 include a succinct FET clause without an interpretative explanation of its application, it ultimately depends on the arbitral tribunals to interpret these simple FET clauses. These simple FET clauses in Chinese IIAs do not contain explanatory text that effectively excludes the "minimum standard of treatment" or "legitimate expectations" (e.g. clauses that say "the mere fact that a Party takes or fails to take an action that may be inconsistent with an investor's

[106] *Agreement on Encouragement and Reciprocal Protection of Investments Between the Government of the People's Republic of China and the Government of the Kingdom of the Netherlands*, 26 November 2001 (entered into force 1 August 2004), art. 3.1.

[107] KONG Qingjiang, "Bilateral Investment Treaties: The Chinese Approach and Practice", in B.S. CHIMNI, KO Swan Sik, Masahiro MIYOSHI, M.C.W. PINTO, Surya SUBEDI, eds., *Asian Yearbook of International Law*, Vol. 8 (Leiden: Brill, 2003), 105 at 123.

[108] China-Canada BIT (2012), *supra* note 104 at art. 4.

[109] *Free Trade Agreement Between the Government of the Republic of Mauritius and the Government of the People's Republic of China*, 17 October 2019 (entered into force 1 January 2021) [*China-Mauritius FTA (2019)*]. Article 8.5 of the China-Mauritius FTA (2019) provides that "each Party shall accord to covered investments fair and equitable treatment and full protection and security in accordance with customary international law." "The concepts of 'fair and equitable treatment' and 'full protection and security' do not require treatment in addition to or beyond that which is required by [the minimum standard of treatment], and do not create additional substantive rights". "'[F]air and equitable treatment' includes the obligation not to deny justice in criminal, civil, or administrative adjudicatory proceedings in accordance with due process of law". "...[T]he mere fact that a Party takes or fails to take an action that may be inconsistent with an investor's expectations does not constitute a breach of [FET] even if there is loss or damage to the covered investment as a result, and the interpretation of FET provision shall accord to customary international law."

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

expectations does not constitute a breach of FET")[110] in guiding a tribunal's interpretation. As a result, foreign investors as claimants may argue, and subsequently arbitral tribunals may support, a breach of FET on multiple grounds. Investors may argue that China's mandatory data sharing constitutes a fundamental breach of due process and transparency, manifests arbitrariness, deprives investors of their legitimate expectations (e.g. due to the lack of legal certainty and predictability in these national measures), or violates the minimum standard of treatment as customary international law. This is not to argue that tribunals will necessarily support such claims by foreign investors or decide in favour of investors; some claims may be dismissed at the decision on jurisdiction phase and not even enter the discussion on their merits. The process and the outcome will be highly dependent on the factual circumstances and the disposition of a tribunal. However, it is at least safe to say that there is an obvious inconsistency between China's mandatory business-to-government data sharing scheme and China's treaty obligations in granting foreign investors FET in its massive investment treaty programme, which creates some potential for investment arbitration claims. In particular, the argument about legitimate expectations and a minimum standard of treatment may create the most problems, such as frivolous claims, inconsistency, and the unpredictability of outcomes.

2. Indirect expropriation

Chinese IIAs that follow a European style also provide a succinct expropriation clause. A typical expropriation clause, such as those found in the Germany-China BIT (2003), reads:

> Investments by investors of either Contracting Party shall not directly or indirectly be expropriated, nationalized or subjected to any other measure the effects of which would be tantamount to expropriation or nationalization in the territory of the other Contracting Party (hereinafter referred to as expropriation) except for the public benefit and against compensation.[111]

It is clear from the wording that expropriatory acts include direct, indirect, and any other measures tantamount to them. These stipulations are also adopted in other IIAs and lead a number of tribunals "to provide the broadest protection for the investments of foreign investors who may suffer harm by being deprived of their fundamental investment rights".[112] Other Chinese IIAs that follow a European style demonstrate variations in language but result in the same effect, for example the China-Peru BIT (1994).[113] Although this BIT does not explicitly include "indirect expropriation", the wording "similar measure" suggests that arbitral tribunals can adopt an expansive interpretation of it to include indirect expropriation.[114]

More recent Chinese IIAs that follow an American style adopt a more elaborate expropriation clause. For example, the China-Peru FTA (2009) uses an annex to explicate the

[110] *Ibid.*

[111] China-Germany BIT (2003), *supra* note 103 at art. 4.2.

[112] Wei SHEN, "Expropriation in Transition: Evolving Chinese Investment Treaty Practices in Local and Global Contexts" (2015) 28 Leiden Journal of International Law 579 at 582.

[113] *Agreement Between the Government of the People's Republic of China and the Government of the Republic of Peru Concerning the Encouragement and Reciprocal Protection of Investments*, 9 June 1994 (entered into force 1 February 1995) [*China-Peru BIT (1994)*]. Article 4.1 of the China-Peru BIT (1994) reads: "Neither Contracting Party shall expropriate, nationalize or take similar measure (hereinafter referred to as 'expropriation') against investments of investors of the other Contracting Party in its territory, unless the following conditions are met: (a) for the public interest; (b) under domestic legal procedure; (c) without discrimination; (d) against compensation."

[114] Shen, *supra* note 112 at 583.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

scope of indirect expropriation.[115] Even more clarification on indirect expropriation is brought to newer Chinese IIAs such as the China-Canada BIT (2012) and the China-Mauritius FTA (2019), which largely emulate the US Model BIT. Therefore, Chinese IIAs that follow an American style regard a substantial deprivation of investors' property rights as an indispensable condition for the act of indirect expropriation and explicitly distinguish between a state's legitimate regulatory measures and the act of expropriation. However, such treaty provisions in China's entire IIA regime are more of an exceptional case rather than a norm.

As previously discussed, a number of national measures relating to data, such as mandatory business-to-government data sharing, deliberate cyberattacks orchestrated by the state, and data localization requirements, could also give rise to expropriation claims. To determine the existence of indirect expropriation, arbitral tribunals have developed different approaches if the investment treaty in question does not provide clear interpretative guidance, as is the case in the majority of Chinese IIAs that follow a European model. If a tribunal considers an investor's legitimate expectations or the economic impact of a state measure as an element in determining indirect expropriation, potential breaches may be found. Taking China's data localization rules as an example, foreign investors could argue that data localization laws and measures have either drastically increased the cost of tech companies doing business in China or have substantially deprived the investors' ability to make a profit out of the value of data if data cannot be transferred across borders, thus causing anticipated or actual losses in economic benefit or a negative economic impact.

Other tribunals have attempted to introduce a test of proportionality analysis (or some parts of it) in determining indirect expropriation, which may involve four analytical stages that include legitimacy, suitability, necessity, and strict proportionality.[116] In this event, investors could argue that China's data localization laws and measures are too broad and intrusive on businesses to achieve the generic proclaimed goals of protecting cyber security, data security, or privacy, leading to a claim that measures on data localization are disproportionate to their regulatory goal and may constitute indirect expropriation.

Last but not least, there has been a rise in claims globally on regulatory expropriation or creeping expropriation: a law or measure or a progression of laws and measures adopted by the host state that do not target a particular investor or a group of investors but nevertheless have a negative impact on the economic value of the investment or negatively affect investors' legitimate expectations.[117] As the majority of Chinese IIAs do not contain language with the effect of excluding legitimate regulatory measures from acts of expropriation, foreign investors could make a claim of regulatory or creeping expropriation when there is a modification of data laws or the promulgation of new data laws that prohibit or restrict further cross-border data transfer in China. In this event,

[115] *Free Trade Agreement Between the Government of the Republic of Peru and the Government of the People's Republic of China*, 28 April 2009 (entered into force 1 March 2010) [*China-Peru FTA (2009)*]. Annex 9 of the China-Peru FTA (2009) reads: "indirect expropriation occurs when a state takes an action or series of action that have an effect equivalent to direct expropriation, in that it deprives the investor in substance of the use of the investor's property", "[i]n order to constitute indirect expropriation, the action or series of actions must be: (a) either severe or for an indefinite period; and (b) disproportionate to the public interest", the determination of indirect expropriation should "consider the economic impact of the government action", and except in rare circumstances [discriminatory in its effect or in breach of state's prior binding written commitment to the investor], "measures taken in the exercise of a state's regulatory powers as may be reasonably justified in the protection of the public welfare, including public health, safety and the environment, shall not constitute an indirect expropriation."

[116] Henckels, *supra* note 61.

[117] Isakoff, *supra* note 56 at 194–6.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

China, as the host state, could cite the public interest prerogative in the expropriation clause in a treaty or the police powers doctrine as a general principle of international law as defence, although "arbitral tribunals have struggled to distinguish state police powers from compensable expropriation, especially indirect expropriation", and this has resulted in inconsistent outcomes.[118] In short, China's data localization laws and practices may give rise to claims of expropriation especially when the IIA in question follows a traditional succinct European model that does not explicitly exclude several grounds for an expropriatory claim.

C. Data Residency Provisions in the RCEP

Prior to the RCEP, Chinese FTAs have not dealt with cross-border data flows, presumably because "China is concerned that commitments to free flow of information for e-commerce in the FTAs will ultimately make its internet censorship a trade barrier".[119] The RCEP remains the first and only FTA to which China is a party that includes a chapter on cross-border data flows, which also applies to the investment chapter. The RCEP stipulates that: "[n]o Party shall require a covered person (an investor and its investment under the investment chapter) to use or locate computing facilities in that Party's territory as a condition for conducting business in that Party's territory" unless it is necessary to achieve a legitimate public policy objective, provided that the measure does not constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade, or unless it is for the protection of essential security interests and "(a) Party shall not prevent cross-border transfer of information by electronic means where such activity is for the conduct of the business of a covered person" unless it is necessary to achieve a legitimate public policy objective, provided that the measure does not constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade, or unless it is for the protection of essential security interests.[120]

In addition to the above-mentioned data localization laws that restrict the free flow of personal and important data, China also maintains a rigorous censorship of the Internet, known as the "Great Firewall", which filters online content and restricts data flow both into and out of Chinese territory.[121] China also imposes a requirement for the localization of computing facilities within the country, which covers a wide range of the economy. For example, online publishing service providers operating in China must locate their servers and storage devices in China.[122] Therefore, it appears that the treaty obligation on the prohibition of localization of computing facilities and prohibition on cross-border data transfer in the RCEP would restrict the scope of Chinese domestic law in establishing data localization rules and restrictions on the free flow of data across national boundaries. However, these treaty obligations do not go very far because regulations on data residency remain a sovereign prerogative as long as they are for a legitimate public policy purpose in the context of the RCEP. For China, data localization rules can always be justified by a public purpose, such as the

[118] *Ibid.*, at 193.

[119] Jie HUANG, "Comparison of E-commerce Regulations in Chinese and American FTAs: Converging Approaches, Diverging Contents, and Polycentric Directions?" (2017) 64 Netherlands International Law Review 309 at 323.

[120] RCEP (2020), *supra* note 105 at arts. 12.14 and 12.15.

[121] For a comprehensive discussion, see Jyh-An LEE and Ching-U LIU, "Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China" (2012) 13(1) Minnesota Journal of Law, Science and Technology 125.

[122] Huang, *supra* note 119 at 328–9.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

protection of data security, "combat[ing] rampant identity theft and diminish illegal trade in personal data" or the protection of China's socialist, political, and ideological values.[123] The public policy derogation in the data residency provisions of the RCEP leaves ample leeway for the contracting states to adopt or amend national laws on data localization.

Nevertheless, the RCEP may pose a significant impact and bring a paradigm shift to China's future IIA-making with respect to data residency and governance. Although China has the world's second largest IIA regime, second only to Germany,[124] the majority of its IIAs were concluded between the 1990s and 2000s and do not incorporate provisions on data residency. Being the very first comprehensive trade and investment agreement, China is a party of on data residency; the RCEP could serve as a template for China in future IIA negotiations that address data residency. Furthermore, considering that Chinese IIAs in general provide for Most-Favoured-Nation treatment, there is also a possibility for foreign investors to refer to data residency provisions in the RCEP and extend them to investments covered by other Chinese IIAs.

V. Conclusion

Data plays a fundamental and pivotal role in the digital economy. With China's exceptional performance in the digital economy, in combination with its allure as a destination to attract foreign investment, it is anticipated that data-based and data-related investment will gain considerable momentum in growth. Meanwhile, China's IIA regime appears to contain a dichotomy that creates both a facilitation and an encumbrance to different stakeholders.

To foreign investors, Chinese IIAs appear to generate more facilitation than impediments in resorting disputes relating to data to international investment arbitration. First, as almost all Chinese IIAs adopt a broad definition of a covered investment – predominately as "every kind of assets" – data as a covered investment and a subject under the treaty protection is in theory permissible. With regard to substantive standards of protection in Chinese IIAs, China's domestic law on data governance appears to have the potential to give rise to a number of claims of treaty breaches. China adopts and implements, at both the central and local levels, laws, policies, and practices pertinent to mandatory business-to-government data sharing, data localization requirements, prohibitions and restrictions on data transfer to overseas territories, internet censorship or content restrictions, and so on. A common theme of these laws, policies, and practices is that they are broad in their scope of application, often lack specified procedures on how these rules are enforced, involve a significant amount of government discretion, may be arbitrary or opaque in enforcement, lack administrative or judicial remedies in cases of encroachment of private interests, or may be disproportionate for achieving proclaimed goals such as data sovereignty or cybersecurity.

These characteristics may easily collide with substantive standards of protection in Chinese IIAs such as FET or indirect expropriation. As the overwhelming majority of Chinese IIAs follow a succinct European style that does not clarify the interpretative margin of these substantive standards of protection, investors may attempt to, or at least are not restricted by treaty language, make a claim in ISDS against China's various data-related laws, policies, and measures once their investment suffers actual or anticipated loss. This of course does not guarantee the tribunals' confirmation on jurisdiction,

[123] *Ibid.*

[124] Yuwen LI and Cheng BIAN, "China's Stance on Investor-State Dispute Settlement: Evolution, Challenges, and Reform Options" (2020) 67 Netherlands International Law Review 503 at 504.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

much less a favourable outcome for the investor. But at least investors are offered an additional possibility to resort to international investment arbitration to challenge national laws, policies, and practices on mandatory data sharing and the impediment to a free flow of data, which would be impossible as a legal remedy within the Chinese domestic legal and judicial system.

To China as a host state, however, the IIA regime may become an excessive burden that puts too much emphasis on investors' protection but not enough on the host state's right to regulate. As the vast majority of Chinese IIAs adopt a European model of BIT making, which includes standard repertoires of substantive standards of protection in rather succinct text – such as FET, full protection and security, non-discrimination, minimum standards of treatment, and provisions on expropriation – their interpretative margin and scope of application are not at all certain and are subject to the interpretation of *ad hoc* arbitral tribunals. Some more recent Chinese IIAs, such as the China-Mauritius FTA (2019) and the China-Canada BIT (2012), are more mindful of the host state's regulatory spaces and prerogatives, which include treaty language with greater precision, which is on a par with global new generation IIAs. This treaty negotiating strategy is of course a positive development and a step in the right direction, but its representation in China's large IIA regime is still rather marginal. So far, RCEP is the only IIA to which China is a party that includes a chapter on cross-border data flows and data residency, but its treaty obligations on the free flow of data and prohibition on data localization do not go very far. As a result, data-related investment disputes may become a new frontier in the future for foreign investors to challenge the Chinese government over its domestic data laws, policies, and measures in international investment arbitration. As the Chinese government seeks to avoid the possibility of being a frequent respondent in ISDS, Chinese IIAs may pose an encumbrance to that effect in the context of data-related foreign investment disputes.

In conclusion, there is a duelling incompatibility between China's data governance that is in principle stringent and restrictive and emphasizes data sovereignty and security and Chinese IIAs that, in general, make sweeping commitments to investors for protection and access to ISDS, giving rise to potential investor-state disputes relating to data. A fundamental reason for such an incompatibility is that the majority of Chinese IIAs were formulated from the early 1980s to the early 2010s, but still remain in effect today, while China's domestic data laws and policies only began to take shape around the late 2010s, which means IIAs previously concluded may no longer accommodate new legislative developments at the domestic level. For China to address this incompatibility at the international law level there is a need for an update to and modernization of the previous generations of Chinese IIAs in order to strike the right balance between the liberalization of data flow across national boundaries in the digital age and the promotion of domestic policy goals on data governance relating to security and privacy. At the national level, legislators should be more mindful of the ways in which laws, policies, and measures on data governance are formulated or evolved in order to be on par with China's IIA commitments to protect foreign investors. A general framework for the desired reform of both international and national law in the future should aim at establishing an open and efficient environment for cross-border data transfer on the one hand and secure and transparent data governance to eliminate cyber risks and protect digital assets on the other. Noting that this article only discusses this incompatibility on a theoretical basis, future research could further investigate the investment arbitration practice and jurisprudence if investor-state disputes arise with regard to China's data governance.

Acknowledgements. The author would like to thank the reviewers for their comments.

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press

Funding statement. None.

Competing interests. The author declares none.

Dr Cheng BIAN is an Assistant Professor at the Erasmus School of Law, Erasmus Universiteit Rotterdam, Netherlands.

Cite this article: BIAN C (2023). Data as Assets in Foreign Direct Investment: Is China's National Data Governance Compatible with its International Investment Agreements? *Asian Journal of International Law* **13**, 342–364. https://doi.org/10.1017/S2044251322000595

https://doi.org/10.1017/S2044251322000595 Published online by Cambridge University Press