Published in Journal of World Investment & Trade (2023) 24 (2), 256-300. DOI: 10.1163/22119000-12340288

Regulating Artificial Intelligence in International Investment Law

Mark McLaughlin | ORCID: 0000-0002-3173-5670
School of Law, Singapore Management University, Singapore, Singapore
mmclaughlin@smu.edu.sg

Abstract

The interaction between artificial intelligence (AI) and international investment treaties is an uncharted territory of international law. Concerns over the national security, safety, and privacy implications of AI are spurring regulators into action around the world. States have imposed restrictions on data transfer, utilised automated decision-making, mandated algorithmic transparency, and limited market access. This article explores the interaction between AI regulation and standards of investment protection. It is argued that the current framework provides an unpredictable legal environment in which to adjudicate the contested norms and ethics of AI. Treaties should be recalibrated to reinforce their anti-protectionist origins, embed human-centric AI principles, and embrace expert witnesses and amicus briefs.

Keywords

artificial intelligence – digital economy – international investment law – international law and technology – investment arbitration

1 Introduction

Artificial Intelligence (AI) is emerging as a significant phenomenon in the global economy. As multinational corporations pour capital into acquiring AI start-ups, investment in cognitive AI systems is expected to reach

USD 98 billion by 2023.[1] The United States and China have established initiatives to pursue strategic dominance of AI,[2] while several other developed countries are nurturing their own AI sectors.[3] Such is the promise of creative destruction associated with AI that the concept of privacy, the nature of work, the accountability of governments, and the value of data must all be reviewed in response to AI-driven technological advancements. Indeed, concerns about the ensuing public interest implications have provoked a series of responses by national legislatures as States attempt to fill the regulatory vacuum.[4]

While international economic law literature is becoming increasingly cognisant of AI, the interaction between AI and investment treaties remains uncharted territory.[5] Scholars have addressed how AI will exacerbate the 'digital divide' within cross-border trade,[6] contribute to data-driven research within international economic law,[7] and even generate treaties to predict the outcome of negotiations.[8] Broader issues of international arbitration have similarly been scrutinized within the context of AI, for predicting outcomes, selecting arbitrators, and calculating damages.[9] In contrast, AI's interaction

[1] International Data Corporation (IDC), 'Worldwide Artificial Intelligence Spending Guide' (IDC, 2019) <www.idc.com/tracker/showproductinfo.jsp?containerId=IDC_P33198> accessed 3 November 2021.

[2] For China, see State Council, 'The Next Generation of Artificial Intelligence Development Plan' (2017) State Council Document 35. For the United States, see Executive Office of the President and National Science and Technology Council Committee on Technology, 'Preparing for the Future of Artificial Intelligence: A Government Report' (2016).

[3] For example, see Wendy Hall and Jérôme Pesenti, 'Growing the Artificial Intelligence Industry in the UK' (Independent Report, Department for Digital, Culture, Media and Sport – Department for Business, Energy and Industrial Strategy, 2017); Cédric Villani and others, 'For a Meaningful Artificial Intelligence: Towards a French and European Strategy' (Conseil national du numérique, 2018).

[4] A Atabekov and O Yastrebov, 'Legal Status of Artificial Intelligence Across Countries: Legislation on the Move' (2018) XXI European Research Studies Journal 773.

[5] Shin-Yi Peng, Ching-Fu Lin and Thomas Streinz (eds), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (CUP 2021); Han-Wei Liu and Ching-Fu Lin, 'Artificial Intelligence and Global Trade Governance: A Pluralist Agenda' (2020) 61 Harv Intl L J 407.

[6] Susan Ariel Aaronson and Patrick Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21 JIEL 245; Henry Gao, 'Digital or Trade? The Contrasting Approaches of China and US to Digital Trade' (2018) 21 JIEL 297.

[7] Wolfgang Alschner, Joost Pauwelyn and Sergio Puig, 'The Data-Driven Future of International Economic Law' (2017) 20 JIEL 217.

[8] Wolfgang Alschner and Dmitriy Skougarevskiy, 'Can Robots Write Treaties? Using Recurrent Neural Networks to Draft International Investment Agreements' (2016) 294 Legal Knowledge and Information Systems.

[9] Christine Sim, 'Will Artificial Intelligence Take Over Arbitration?' (2018) 14 Asian International Arbitration Journal 1.

with investment treaties has garnered little attention, and is the focus of this article.

The central thesis is that the international investment regime provides an unpredictable legal environment in which to adjudicate the emerging norms and ethics of AI. Reforms to drafting and to practice are necessary to prepare investment treaties for an AI-driven future.

This article proceeds in five Sections. Section 2 considers the components and regulation of AI. It is argued that AI regulation – including limitations on market access, utilization of automated decision-making systems, restrictions on cross-border data flows, and mandated algorithmic transparency – may constitute barriers to investment. Section 3 discusses the conditions for AI to be within the scope of protected investment in international investment agreements (IIAs). Section 4 analyses whether measures targeting AI are in compliance with substantive investment obligations. Having identified areas of potential breach, Section 5 finds that existing exceptions clauses within IIAs are too narrowly drafted to encompass the relevant policy concerns. As a result, Section 6 proposes three reformative measures to optimize investment treaties for the AI-powered investor and AI-powered host State.

2 The Components and Regulation of Artificial Intelligence

There is no consensus on a definition for AI.[10] It has been defined in four different ways, as computer programs capable of: acting humanly, thinking humanly, thinking rationally and acting rationally.[11] None offer a suitably firm basis on which to frame regulation.

The former two categories define AI in relation to human characteristics that are themselves indefinable. What is learning? What is self-awareness? What is reasoning? It is impossible to define these terms with enough precision to identify targets of regulation. The third approach, 'thinking rationally', is likely to be over-inclusive, as even rudimentary algorithms follow logical laws of thought. Finally, the 'acting rationally' approach defines AI by its ability to operate autonomously, adapt to changing circumstances, and pursue goals.[12] The notion of AI as a 'rational agent' has proven to be the most influential approach in the field.

[10] John McCarthy, 'What Is AI?' (2007) <http://jmc.stanford.edu/articles/whatisai.html> accessed 3 November 2022.

[11] Stuart J Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Global edn, Pearson 2021) 19–22.

[12] ibid; David Poole, Alan Mackworth and Randy Goebel, *Computational Intelligence: A Logical Approach* (OUP 1998).

However, two aspects of this definition remain challenging. Firstly, assessing whether a computer program is 'pursuing' a 'goal' involves allusions to intent and consciousness, which creates the same ambiguity that exists with imitating indefinable human characteristics.[13] Secondly, perceptions of autonomy are highly subjective.[14] They rely upon our perceptions of foreseeability that necessarily shift as the technology becomes more familiar. Indeed, as John McCarthy remarked, 'as soon as it works, no one calls it AI any more'.

Therefore, this article will forego any attempt to define AI from a technical perspective. Instead, it will adopt a normative approach based upon regulations in development in the EU and the United States. The proposed EU AI Act defines an AI system as 'software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with'.[15] Similarly, the US Algorithmic Accountability Act defines an 'automated decision system' as 'a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making, that impacts consumers'.[16]

AI regulation is being constructed around certain techniques and technologies, and the risks they pose to those with whom they interact. Similarly, international investment law protects and regulates certain assets, activities, and public interests. Therefore, recognizing the points at which AI intersects with investment law will involve identifying the assets, activities and public interest implications, or risks, of AI. As a first step, this requires identifying its components and applications.

[13] Matthew U Scherer, 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies' (2016) 29 Harv J L & Tech 354; Miriam C Buiten, 'Towards Intelligent Regulation of Artificial Intelligence' (2019) 10 EJRR 41.

[14] Buiten (n 19) 44.

[15] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (21 April 2021) 2021/0106 (COD) art 3; Annex I contains techniques or technology associated with AI: 'Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods'.

[16] Section 2(1) Algorithmic Accountability Act of 2019, s 1108, 166th Cong (US) (2019).

2.1 *The Components and Applications of Artificial Intelligence*

2.1.1 Components of Artificial Intelligence

AI systems have varying degrees of complexity and different risk profiles. However, there are three components that can be used to assess the interaction with the investment regime: algorithms, data, and (sometimes) physical hardware.

Simple AI systems contain an algorithm – a computer code that contains specific rules or instructions – that controls how the program should analyse and act upon input data. The archetypal example is a system designed to play chess: it evaluates all possible moves using a scoring system inputted by the programmer.[17] For a more complex system, there are two interacting algorithms: a control algorithm, which provides the original parameters of action (in the chess example, the preplanned scoring system) and a learning algorithm, that can change this scoring system based upon what move is most effective in its 'experience' (including playing against itself) when it encounters novel situations.[18] The complex AI system evolves its parameters based on patterns identified in the data by the learning algorithm.

The second relevant component of AI systems is flows of data.[19] Complex AI systems involve a feedback loop whereby training data and the AI algorithms interact. In 2019, a global survey of data scientists, AI experts, and stakeholders found that the vast majority considered that AI projects must be tested by at least 100,000 data items in order to be deployed with confidence.[20] However, over half of the respondents indicated that 'not enough data' was an obstruction to AI projects. Advancements in AI are fueled by access to large datasets, and the continuous flow of data.

Thirdly, many AI systems involve some physical hardware, which is often an extremely high value element of AI. Prominent examples include autonomous vehicles, unmanned drones, or robotic limbs. Not all AI systems will

[17] Dave Gershgorn, 'Artificial Intelligence Is Taking Computer Chess Beyond Brute Force' (*Popular Science*, 18 March 2019) <www.popsci.com/artificial-intelligence-takes-chess-beyond-brute-force/> accessed 3 November 2022.

[18] Deven R Desai and Joshua A Kroll, 'Trust but Verify: A Guide to Algorithms and the Law' (2017) 31 Harv J L & Tech 2, 27.

[19] Daniel E O'Leary, 'Artificial Intelligence and Big Data' (2013) 28 IEEE Intelligent Systems 96.

[20] 'Artificial Intelligence and Machine Learning Projects Are Obstructed by Data Issues Global Survey of Data Scientists, AI Experts and Stakeholders' (Dimensional Research, May 2019) <https://cdn2.hubspot.net/hubfs/3971219/Survey%20Assets%201905/Dimensional%20Research%20Machine%20Learning%20PPT%20Report%20FINAL.pdf> accessed 3 November 2022.

have unique hardware, but it is often developed in conjunction with AI software and forms an integral part of the overall system.

To assess how AI is being regulated, and whether AI is protected under investment law, it is necessary to examine how these components are treated within domestic legal systems and investment treaties. Regulation will be informed by AI's applications in public administration, the military, industry, and consumer goods.

2.1.2 Applications of Artificial Intelligence

States are increasingly utilizing AI as part of public service provision.[21] In the United States, authorities are trialing predictive algorithms to assess the likelihood that a person will re-offend.[22] In China, advanced facial recognition technology is being utilised in the name of improving security.[23] 'Predictive analytics' are being used in Canada as part of decisions on the status of immigrants and refugees.[24]

Governments are embedding AI to advance military capabilities.[25] The most prominent example is perhaps unmanned aircraft, which are already in use. In other cases, AI is being integrated with existing military and intelligence infrastructure. For example, real-time translations and imagery analysis can be used to reduce the manpower necessary to carry out certain supportive roles, and perform with a higher degree of accuracy.[26] This includes drastically improving capabilities to commit cyber-attacks and improve cyber-defenses.

Outside government, AI will be transformative within industrial contexts. Machine learning AI may provoke a reassessment about the role of human decision-making and manual labour within global value chains.[27] At present,

[21] Bernd W Wirtz, Jan C Weyerer and Carolin Geyer, 'Artificial Intelligence and the Public Sector – Applications and Challenges' (2019) 42 International Journal of Public Administration 596.

[22] Julia Dressel and Hany Farid, 'The Accuracy, Fairness, and Limits of Predicting Recidivism' (2018) 4(1) Science Advances (online).

[23] Brett Aho and Roberta Duffield, 'Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China' (2020) 49 Economy and Society 187, 192.

[24] Petra Molnar and Lex Gill, 'Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System' (2018) Citizen Lab and International Human Rights Program <https://tspace.library.utoronto.ca/handle/1807/94802> accessed 3 November 2022.

[25] Alina Polyakova, 'Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare' (*Brookings*, 15 November 2018).

[26] Justin Haner and Denise Garcia, 'The Artificial Intelligence Arms Race: Trends and World Leaders in Autonomous Weapons Development' (2019) 10 Global Policy 331.

[27] Nick Crafts and others, 'The Impact of Artificial Intelligence on Work: An Evidence Synthesis on Implications for Individuals, Communities, and Societies' (British Academy

it is technology firms that are investing significantly in AI, but productivity gains may be most realizable in the manufacturing sector.[28] The ability to increase efficiencies and align supply with demand will improve the viability of just-in-time delivery systems and advancements in robotics will impact manufacturing, packing, and quality assurance.[29]

However, the average person will most commonly encounter AI as part of everyday consumer goods and services. Voice commands issued to Apple's 'Siri' and Amazon's 'Alexa' attempt to simulate human interaction, with speech-recognition technology facilitating access to other devices and services.[30] AI is powering Google's search engine to understand the context of words instead of searching for terms one-by-one.[31] Machine learning underpins Netflix's systems of personalization.[32] Alphabet, Tesla and General Motors have reportedly invested billions of dollars to develop machine learning and deep learning architectures for the development of autonomous vehicles.[33]

The applications of AI in public services, the military, industry, and consumer goods are increasingly the target of government regulation.

2.2 *Artificial Intelligence Regulation and Possible Investment Barriers*

The regulation of AI can be divided into four categories: limitations on market access, restrictions on the collection, transfer, or storage of data, the use of automated decision-making, and mandates for algorithmic transparency. All create barriers to cross-border investment and trade. Such measures are a response to concerns over the nature of AI technology and the effect that AI will have on global economic governance.

for the Humanities and Social Sciences, The Royal Society, 2018) <www.thebritishacademy.ac.uk/documents/280/AI-and-work-evidence-synthesis.pdf> accessed 3 November 2022.

[28] Justin Shields, 'Smart Machines and Smarter Policy: Foreign Investment Regulation, National Security, and Technology Transfer in the Age of Artificial Intelligence' (2018) 51 J Marshall L Rev 279, 282.

[29] Dani Rodrik, 'New Technologies, Global Value Chains, and Developing Economies' (National Bureau of Economic Research, 2018) Working Paper 25164.

[30] Gustavo López, Luis Quesada and Luis A Guerrero, 'Alexa vs. Siri vs. Cortana vs. Google Assistant: A Comparison of Speech-Based Natural User Interfaces' in Isabel L Nunes (ed), *Advances in Human Factors and Systems Interaction* (Springer 2018) 241.

[31] Prabhakar Raghavan, 'How AI Is Powering a More Helpful Google' (Google, 15 October 2020) <https://blog.google/products/search/search-on/> accessed 3 November 2022.

[32] Netflix Research, 'Machine Learning: Learning How to Entertain the World' <https://research.netflix.com/research-area/machine-learning> accessed 3 November 2022.

[33] Aarian Marshall, 'Robocars Could Add $7 Trillion to the Global Economy' (*Urbanism Next*, 2017) <www.urbanismnext.org/resources/robocars-could-add-7-trillion-to-the-global-economy> accessed 3 November 2022.

Firstly, there is an intense zero-sum dynamic in the data-driven economy, of which AI is a significant part. The considerable capital required to develop AI coupled with the comparatively low cost of expanding or replicating existing systems produces a strong first-mover advantage.[34] Unlike traditional neoliberal orthodoxy, whereby economic cooperation is assumed to produce mutual benefit, the emerging paradigm may encourage protectionism when barriers to investment are considered to enhance competitiveness.[35] This is not to assert that the nature of AI is determinative of a universally protectionist turn in data regulation – the proposed EU Data Act mandates data-sharing to preserve competition – only that restrictions on cross-border data transfer or foreign acquisitions of technology might be adopted to protect a perceived comparative advantage.[36]

Secondly, AI and its associated data flows pose security concerns. Military technologies and the protection of defense-related sensitive data are the most obvious example of these concerns. However, the hybrid civilian/military applications of AI may create additional complications. For example, Project Maven involved employees at Google developing computer-vision algorithms that might be used in warfighting systems.[37] AI will also engage non-traditional areas of national security such as 'precision propaganda' and 'deep fakes' – simulated video footage that is almost indistinguishable from real video – that could undermine trust in institutions and foment social unrest.[38] This has been described as 'AI-driven asymmetric warfare'[39] that is causing the 'erosion of the distinction between war and peace and the emergence of a grey zone'.[40]

[34] Dan Ciuriak, 'Industrial-Era Investment Strategies Won't Work in a Data-Driven Economy' (Centre for International Governance Innovation, 15 November 2018).

[35] In China, the State Council's 2015 Action Plan for Promoting Big Data Development expressly references the goal of leveraging China's 'data scale advantage'. Notice of the State Council, 'Issuing the Action Outline for Promoting the Development of Big Data' (31 August 2015) Document No 50 <http://lawinfochina.com/display.aspx?id=26624&lib=law> accessed 3 November 2022.

[36] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data' (23 February 2022) (Data Act) 2022/0047/COD.

[37] Dell Cameron and Kate Conger, 'Google Is Helping the Pentagon Build AI for Drones' (*Gizmodo*, 3 June 2018) <https://gizmodo.com/google-is-helping-the-pentagon-build-ai-for-drones-1823464533> accessed 3 November 2022.

[38] Polyakova (n 31).

[39] ibid.

[40] Keir Giles, 'The Next Phase of Russian Information Warfare' (NATO Strategic Communications Centre of Excellence, 2016) 4 <https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176> accessed 3 November 2022.

Thirdly, AI may have far-reaching implications for human rights, in particular the right to privacy, the right to non-discrimination, and due process obligations.[41] AI systems can identify individuals from supposedly anonymized metadata, which, at best, constitutes a breach of privacy, and at worst, could pose a threat to political dissidents.[42] If AI is trained by discriminatory data, or insufficient data, it may also produce discriminatory outcomes; Amazon has abandoned a recruiting tool that downgraded female applicants,[43] and Google removed the terms 'chimpanzee' and 'gorilla' from its photo labelling systems after pictures of African-Americans were labelled as such.[44] The potential for discrimination is exacerbated by the 'black box' nature of some AI – it is not always apparent, even to the programmer, why the AI comes to its conclusion or how certain factors are weighed up in reaching its decision. Given that due process commonly includes a right to reasons, the integration of advanced AI within public service provision poses obvious public policy concerns. These concerns are driving AI-related regulatory measures.

2.2.1 Limitations on Market Access

Several States restrict market access in relation to AI. Perhaps the most remarked-upon is the Committee for Foreign Investment in the United States (CFIUS), the scope of which has been expanded to include non-controlling interests in critical technologies and security-sensitive personal data.[45] Recent updates to CFIUS also require a biennial report into patterns of Chinese investment in the context of the 'Made in China 2025' plan, suggesting a conflation of economic and security reviews of investment.[46] Similarly, the Investment Canada Act establishes that any review of an investment must incorporate a test of its effect on 'the transfer of sensitive technology or know-how'.[47] In the case of Japan, the Ministry of Economy, Trade, and Industry has issued a

[41] Karl Manheim and Lyric Kaplan, 'Artificial Intelligence: Risks to Privacy and Democracy' (2019) 21 Yale Journal of Law & Technology 106; Liu, Lin and Chen (n 5).

[42] Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 IDPL 74.

[43] Jeffrey Dastin, 'Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women' (*Reuters*, 11 October 2018) <www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G> accessed 3 November 2022.

[44] Tom Simonite, 'When It Comes to Gorillas, Google Photos Remains Blind' (*Wired*, 22 January 2018) <www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind/> accessed 3 November 2022.

[45] Foreign Investment Risk Review Modernization Act of 2018 (US) (FIRRMA) s 1703(4)(D).

[46] ibid s 1719 (b)(F).

[47] Innovation, Science and Economic Development Canada, 'Guidelines on the National Security Review of Investments' (23 March 2021) art 8(ii) <www.ic.gc.ca/eic/site/ica-lic.nsf/eng/lk81190.html> accessed 3 November 2022.

public notice requiring that acquisitions relating to software for information processing must submit an advance notice to facilitate a security review.[48] While China has included the AI industry in the Catalogue of Industries for Encouraged Investment, and therefore does not adopt overt market access restrictions, allegations persist that it operates a 'technology for access' policy, which inevitably has practical implications for potential AI investors.[49]

2.2.2 Restrictions on Data Flows

Restrictions on the cross-border transfer of data can fall into one of three categories.[50] The first category is the most stringent: measures that mandate the local storage of data. The Chinese data governance regime is a prominent example. It is comprised of the 2017 Cybersecurity Law, the 2021 Data Security Law, and the 2021 Personal Information Protection Law. In many ways, the Chinese data regime attempts to create a form of Chinese sovereignty in cyberspace. It foregrounds national security and utilizes data localization requirements to safeguard perceived national interests. Article 37 of the Cybersecurity Law mandates that 'Critical Information Infrastructure Operators' operating in specific sectors must store data in China.[51] The Data Security Law clarifies that these restrictions are aimed at the 'outbound security management of the important data collected or produced by critical information infrastructure operators', but cross-border data transfer may be permitted in accordance with a request from overseas law enforcement.[52] However, the Personal Information Protection Law appears to adopt a more relaxed approach, permitting transfers if: i) it passes a security assessment by the Cyberspace Administration of China (CAC) ii) the firm obtains a protection certificate from a CAC approved firm or iii) the parties include prescribed contractual language detailing rights

[48] Ministry of Economy, Trade and Industry (METI), 'Addition of Businesses Required to Submit Prior Notification Concerning Inward Direct Investment, Etc.' (27 May 2019) <www.meti.go.jp/english/press/2019/0527_001.html> accessed 3 November 2022.

[49] Julia Ya Qin, 'Forced Technology Transfer and the US–China Trade War: Implications for International Economic Law' (2019) 22 JIEL 743, 755.

[50] Han-Wei Liu and Shin-Yi Peng, 'The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?' (2017) 51 JWT 1, 183; Han-Wei Liu, 'Data Localization and Digital Trade Barriers: ASEAN in Megaregionalism' in Pasha L Hsieh and Bryan Mercurio (eds), *ASEAN Law in the New Regional Economic Order: Global Trends and Shifting Paradigms* (CUP 2019) 373. For an alternative strict/conditional classification, see Martina Ferracane, 'Restrictions on Cross-Border Data Flows: A Taxonomy' (European Centre for International Political Economy, 2017) ECIPE Working Paper No 1/2017.

[51] Cybersecurity Law (China) (1 June 2017) art 37.

[52] Data Security Law of the PRC (10 June 2021) arts 31, 36.

and obligations with respect to the data.[53] It is as yet unclear how these provisions will interact and be implemented, but demonstrate a strong example of 'data sovereignty'.

The second category of measures are those that take a sector-based approach. This approach reflects the fact that different forms of data can have different levels of sensitivity. Restrictions may vary according to whether the data is personal or non-personal. While this is not a straightforward distinction to maintain, it is nevertheless useful for addressing individual sectors. For example, Australian regulations require that the controller of e-health records must not 'process or handle the information relating to the records outside Australia'.[54] Government-controlled personal data is also subject to data localization requirements in Canada,[55] with similar measures being considered in Germany and France.[56]

The third category of measures permit cross-border data transfer, subject to certain conditions. The European Union is the foremost purveyor of this approach, with the General Data Protection Regulation (GDPR). GDPR requires equivalence in national data protection regulation of regular data transfers and may involve consent from the data subject in certain circumstances.[57] Similar rules on equivalence are contained in data protection legislation concluded by Singapore[58] and Malaysia.[59]

2.2.3 Automated Decision-Making

The regulation or use of automated decision-making may constitute barriers to investment in two ways. Firstly, a number of jurisdictions have imposed obligations on providers of digital services relating to the fairness or explainability of their systems. The United States and the European Union have crafted proposals that seek to introduce fairness, transparency, and accountability for firms

[53] Personal Information Protection Law (China) (1 November 2021) art 38.

[54] Personally Controlled Electronic Health Records Act (Australia) (2012) (PCEHR) s 77.

[55] Freedom of Information and Protection of Privacy Act (Canada) (1996) (FIPPA) s 30.1. Personally Controlled Electronic Health Records Act (Australia) (2012) (PCEHR) s 77.

[56] Matthias Bauer and Hosuk Lee-Makiyama, 'The Bundes Cloud: Germany on the Edge to Discriminate Against Foreign Suppliers of Digital Services' (*ECIPE Bulletin*, September 2015) 2; Valéry Marchive, 'Cloud Firms Demand Right to Use French Government's €285m "Sovereign Cloud"' (*ZDNet*, 2 February 2013) <www.zdnet.com/google-amp/article/cloud-firms-demand-right-to-use-french-governments-eur285m-sovereign-cloud/> accessed 3 November 2021.

[57] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, General Data Protection Regulation (4 May 2016) (GDPR) OJ L119, arts 7 and 44–50.

[58] Personal Data Protection Act (Singapore) (2012) s 26(1).

[59] Personal Data Protection Act (Malaysia) (2010) (PDPA) s 129(1) and (2).

employing algorithmic decision-making. The EU Digital Services Act (DSA) specifically targets large online platforms and their content moderation processes.[60] Article 15 of the DSA requires that providers of hosting services that remove or disable access to items of information should provide a 'clear and specific statement of reasons', which must explain the use made of automated means in taking the decision.[61] External oversight requirements are imposed for 'very large online platforms', which must subject their algorithms to an independent audit to assess compliance with obligations relating to illegal content, interference with fundamental rights, or manipulation.[62] While provisions in the US Algorithmic Accountability Act (AAA) are at an earlier stage of development, an independent audit is only required where 'reasonably possible'.[63] Instead, the AAA requires firms of a certain size to undertake an 'automated decision system impact assessment' for the effects on 'accuracy, fairness, bias, discrimination, privacy, and security'.[64]

Secondly, States are embedding automated decision systems within their public service provision, many of which will affect foreign investors. For example, decisions relating to immigration are likely to be of particular significance to foreign nationals. New Zealand and Canada have already incorporated automated systems as part of immigration decisions.[65] Risks to the subjects of these automated decision systems will depend on the weight given to them by the human decision-maker, and the extent to which the decisions are explainable. In such cases, the barrier to investment may not necessarily be the substance of the decision, but the process by which it is taken.

2.2.4 Algorithmic Transparency

The imperative of algorithmic transparency stems from the nature of AI-powered automated decision-making. While AI has the potential to remove unconscious biases and bad faith, and to expedite decision-making, there are also attendant risks of discrimination and threats to public safety. For example,

[60] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC' (15 December 2020) 2020/0361 (COD).

[61] ibid art 15.

[62] ibid art 28.

[63] Section 3(1)(c) of the Algorithmic Accountability Act (US) (2019) (AAA) s 1108, 166th Cong.

[64] ibid s 2(2).

[65] Lucia Nalbandian, 'Canada Should Be Transparent in How It Uses AI to Screen Immigrants' (*The Conversation*, 28 April 2021) <http://theconversation.com/canada-should-be-transparent-in-how-it-uses-ai-to-screen-immigrants-157841> accessed 4 November 2022.

Title IV of the proposed EU AI Act imposes transparency obligations for certain AI systems to take account of their unique potential for manipulation.[66] This includes AI systems that '(i) interact with humans, (ii) are used to detect emotions or determine association with (social) categories based on biometric data, or (iii) generate or manipulate content ('deep fakes')'.[67]

In this context, there are two competing interests: intellectual property rights (IPRs) that protect proprietary information, and the necessity of algorithmic transparency. The internal processes of AI must be open to scrutiny to ensure public safety and public trust. However, such measures may constitute a requirement to transfer technology without safeguards to prevent unauthorized disclosure.

Courts may compel the production of propriety information as part of investigations. This will likely be a common method of disclosure. But the most detailed regulations in this area relate to AI that is used as part of the provision of public services. Canada's Treasure Board Directive on Automated Decision-making has been created to ensure that AI-powered services operate 'in a manner that is compatible with core administrative law principles such as transparency, accountability, legality and procedural fairness'.[68] As part of this effort, source codes must be made available on an Open Resource Exchange and be subject to an Algorithmic Impact Assessment.[69] The approach of the European Union is still in its development stage, but currently imposes an obligation on designers to retain technical data in the course of developing AI for ex-ante assessment.[70] Amsterdam and Helsinki have launched AI registries that provide the datasets used to train AI, an explanation about how the AI is being deployed, and how it was assessed for biases and threats to safety.[71]

[66] Title IV of the European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (21 April 2021) COM(2021) 206 final, 2021/0106 (COD).

[67] ibid 14.

[68] Treasury Board of Canada Secretariat, 'Directive on Automated Decision-Making' (5 February 2019) <www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592> accessed 4 November 2022.

[69] ibid s 6; MIPP, 'Open Resource Exchange' <https://code.open.canada.ca/en/index.html> accessed 4 November 2022.

[70] Artificial Intelligence Act (n 66) art 5.2.3.

[71] Khari Johnson, 'Amsterdam and Helsinki Launch Algorithm Registries to Bring Transparency to Public Deployments of AI' (*VentureBeat*, 28 September 2020) <https://venturebeat.com/2020/09/28/amsterdam-and-helsinki-launch-algorithm-registries-to-bring-transparency-to-public-deployments-of-ai/> accessed 4 November 2022.

These four categories of AI regulation – limitations on market access, restrictions on data flows, automated decision-making, and algorithmic transparency – may constitute entirely rational responses to public policy concerns. However, they may also constitute barriers to investment. To assess whether these barriers are in compliance with investment treaties, it is necessary to establish whether AI is a protected investment.

3 Artificial Intelligence as a Protected Investment

Arbitral tribunals have generally adopted a holistic approach to determining the existence of an 'investment'. As expressed by the Tribunal in *Holiday Inns v Morocco*, '[I]nvestment is accomplished by a number of juridical acts of all sorts. It would not be consonant either with economic reality or with the intention of the parties to consider each of these acts in complete isolation from the others'.[72]

The subject of assessment, therefore, is the 'transaction as a whole'.[73] Investors that utilise AI as part of their provision of goods and services would benefit from investment protection. For example, AI systems used by a healthcare provider to identify cancer cells will likely be protected as part of the overall investment, as the 'disputed activity [is] associated with it in such a way as to bring it under the protection of the Agreement'.[74]

However, for AI-only disputes, such as circumstances in which an investor specifically challenges AI regulation, it may be necessary to establish that the AI itself is a protected investment. In such cases, establishing if AI is a protected investment involves analyzing if its components – algorithms, data, and certain hardware – fall within definitions of 'investment' in IIAs. If the AI investment includes a physical component, like drones or autonomous vehicles, this will likely fall with the scope of most IIAs. The protection of movable or immovable property' or 'tangible or intangible property' has been a fixture of IIAs since the earliest bilateral investment treaties (BITs).[75]

[72] *Holiday Inns, Occidental Petroleum and others v Kingdom of Morocco*, ICSID Case No ARB/72/1, Decision on Problems Raised with Regard to the Connections Between the Basic Agreement and the Loan Contracts (12 May 1974) 3.

[73] *Inmaris Perestroika Sailing Maritime Services GmbH and others v Ukraine*, ICSID Case No ARB/08/8, Decision on Jurisdiction (8 March 2010) CL-52, para 92.

[74] *Bosca v The Republic of Lithuania*, PCA Case No 2011-05, Award (17 May 2013) 166.

[75] Kathryn Gordon and Joachim Pohl, 'Investment Treaties over Time – Treaty Practice and Interpretation in a Changing World' (OECD 2015) OECD Working Papers on International Investment 2015/02, 38.

Conversely, the inclusion of the other components is less clear. The AI system itself, its outputs, and associated data flows require close attention.

3.1 *Artificial Intelligence Systems Are Protected Intellectual Property*

AI-related intellectual property can be divided into three distinct categories: the AI itself, such as a machine-learning algorithm; inventions created by a human who has utilized AI as a tool; and inventions where an autonomous AI has developed something new, absent human input. This section considers the first of these categories.

Since the internationalization of IPRs by the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) in 1995, IPRs have only grown in significance in international economic law.[76] Four methods of incorporation have been identified in IIAs: no explicit reference to IPRs, with reliance on 'assets' or 'property'; inclusion of the term 'intellectual property rights' or 'intangible property' absent further guidance; an express list of covered IPRs such as copyright, trademarks or patents; and a definition of IPRs that may or may not refer to domestic law.[77]

Arbitral cases that directly engage issues of intellectual property remain relatively rare in the context of the investment regime. In those few awards that relate to IPRs, tribunals have taken an inclusive approach to the definition of investment. In 2018, the Tribunal in *A11Y Ltd. V Czech Republic* considered that the provision of 'cutting-edge assistive technologies and holistic solutions for the visually impaired' constituted protected technical know-how and goodwill.[78] Trademarks were at the center of the dispute in *Philip Morris v Uruguay*, in which the Tribunal engaged in an analysis of Uruguayan trademark law as a first step in determining whether there was an investment to be expropriated.[79] In *Bridgestone v Panama*, the Tribunal held that a trademark must be exploited through its use and have the characteristics of an investment.[80] Finally, the Tribunal in *Eli Lilly v Canada* considered the granting and subsequent invalidation of patents granted to a pharmaceutical company to concern an investment.[81]

[76] Bryan Mercurio, 'Awakening the Sleeping Giant: Intellectual Property Rights in International Investment Agreements' (2013) 15 JIEL 871.

[77] Carlos Correa and Jorge E Viñuales, 'Intellectual Property Rights as Protected Investments: How Open Are the Gates?' (2016) 19 JIEL 91.

[78] *A11Y LTD v Czech Republic*, ICSID Case No UNCT/15/1, Award (29 June 2018) 144–46.

[79] *Philip Morris Brands Sàrl, Philip Morris Products SA and Abal Hermanos SA v Oriental Republic of Uruguay*, ICSID Case No ARB/10/7, Award (8 July 2016) 272.

[80] *Bridgestone Americas, Inc and Bridgestone Licensing Services, Inc v Republic of Panama*, ICSID Case No ARB/16/34, Decision on Expedited Objections (13 December 2017) 171–74.

[81] *Eli Lilly and Company v Government of Canada*, ICSID Case No UNCT/14/2, Final Award (16 March 2017) 480.

Arbitral jurisprudence is consistent that IPRs can be a protected investment. The complicating factor is the interaction between domestic law and international law; treaty protection may attach only if the activity is considered an IPR within the domestic law of the contracting parties. However, a limited number of international conventions have established cooperation for IPRs.[82] The Madrid Agreement Concerning the International Regulation of Marks and the Patent Cooperation Treaty establish a process for the filing of protection for trademarks and patents in one jurisdiction to constitute a filing in many.[83] While some inconsistency of practice remains with respect to copyright rules, the Berne Convention for the Protection of Literary and Artistic Works provides some common ground.[84] In contrast, substantial divergences exist concerning the scope and nature of protected trade secrets, despite limited protections for the undisclosed information that has a commercial value within the TRIPS Agreement.[85]

Consequently, if ownership of algorithms or source codes is considered an IPR, AI systems that utilize these elements will qualify as a protected investment. Potential categories of IPR to which they could belong are copyright, patent, and trade secrets.

Practice with respect to recognition of IPRs is not consistent across jurisdictions. The approach of the European Union remains instructive. EU Directive 2009/24 requires that Member States protect computer programs by copyright as literary works within the meaning of the Berne Convention.[86] It requires that the program be 'original in the sense that it is the author's own intellectual creation'.[87] Algorithms and source codes will be considered intellectual property where they demonstrate this originality, with the creator designated as the rightsholder.[88] For AI as an 'invention', the European Patent Office (EPO) considers that computational models and algorithms are mathematical in nature,

[82] Enikő Horváth and Severin Klinkmüller, 'The Concept of "Investment" in the Digital Economy: The Case of Social Media Companies' (2019) 20 JWIT 577, 604.

[83] Madrid Agreement Concerning the International Registration of Marks (14 April 1891) 828 UNTS 389; Patent Cooperation Treaty (19 June 1970) (PCT).

[84] Berne Convention for the Protection of Literary and Artistic Works (4 May 1896) S Treaty Doc No 99-27.

[85] Luigi Alberto Franzoni, 'Trade Secrets Law' in Alain Marciano and Giovanni Battista Ramello (eds), *Encyclopedia of Law and Economics* (Springer 2016) 1 <https://doi.org/10.1007/978-1-4614-7883-6_564-1> accessed 4 November 2022.

[86] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs (Computer Programs Directive) (25 May 2009) OJ L111 16, art 1(1).

[87] ibid art 1(3).

[88] ibid art 2.

and are thus devoid of the technical character essential for patentability.[89] However, this presumption can be overcome when the claimed subject-matter has a 'technical character as a whole'.[90] One example given by the EPO is 'the use of a neural network in a heart-monitoring apparatus for the purpose of identifying irregular heartbeats'.[91] Where an AI system has a technical character, it may be subject to patent protection.

Finally, AI systems may be considered a trade secret. EU directive 2016/943 lays down conditions for 'information' to be so considered: it must (i) be secret, (ii) have commercial value due to its secrecy, and (iii) be subject to reasonable steps to maintain this secrecy.[92]

The definition of investment is inclusive of IPRs, and AI systems can qualify as copyrights, patents, or trade secrets. This may not always be the case with the outputs of AI.

3.2 *Artificial Intelligence 'Inventions' and 'Works': Protection Dependent on Ownership*

Investment protection may attach to the output of AI in certain circumstances. Relevant outputs can be divided into 'inventions' or 'works' created by a human who has utilized AI as a tool, and 'inventions' or 'works' in which an autonomous AI has developed something new, absent human input. Problems of whether or AI can be an 'inventor' is the subject of considerable discussion.[93]

From an investment perspective, the first issue derives from the 'nationality' requirement of IIAs. Definitions of 'investor' routinely require an investment to be made by a national of one party in the territory of another. The nationality of the business or business owner determines the availability of investment protection.

Imagine a US-based AI company that has substantial business operations in Croatia. The US company's AI is used as a tool to invent a new product by a Croatian national in Croatia who is not an employee. If the invention can be

[89] European Patent Office, 'Guidelines for Examination' <www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm> accessed 4 November 2022.

[90] ibid.

[91] ibid.

[92] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure (15 June 2016) OJ L157 1, art 2(1).

[93] Daria Kim, '"AI-Generated Inventions": Time to Get the Record Straight?' (2020) 69 GRUR International 443; Enrico Bonadio, Luke McDonagh and Plamen Dinev, 'Artificial Intelligence as Inventor: Exploring the Consequences for Patent Law' (2021) (1) Intellectual Property Quarterly 48; Michael McLaughlin, 'Computer-Generated Inventions' (2019) 101 Journal of the Patent and Trademark Office Society 224.

patented by the owner of the AI system – the US company – then it will be protected under the US-Croatia BIT, as patents are expressly included within the definition of 'investment'.[94] If it can be patented by the user of the AI system – the Croatian national – then the patent is not held by a national of one party in the territory of another, and it does not meet the *ratione personae* jurisdictional requirements of the BIT.[95] The matter of who can patent the invention should be addressed by their contractual relationship.

The second issue is whether human authorship is a precondition of patent or copyright protection. Consider a computer scientist who develops an AI aimed at autonomously developing 'useful information'.[96] If the output of that AI is patentable and is of a nature that the scientist did not envisage, it is difficult to justify the conclusion that the computer scientist invented it.[97]

Current approaches by the European Patent Office and United States Patent and Trademark Office do not recognize AI as inventors.[98] However, this may not be directly relevant to the investment regime. While inventorship is often the starting point of establishing ownership,[99] most advocates for AI to be recognized as an 'inventor' do not advocate that the system is capable of owning property.[100] If the owner of the AI system retains ownership of its output, then the invention would benefit from the owner's protections under the relevant IIAs. This is the prevailing position within domestic legal systems. Relevant tests include maintaining 'intellectual domination of the work'[101] (United States) and the 'deviser' of an inventive concept (United Kingdom).[102]

[94] US–Croatia BIT (1996) art 1(d)(v).

[95] ibid art 1(e).

[96] Noam Shemtov, 'A Study on Inventorship in Inventions Involving AI Activity' (European Patent Office, 2019) 22 <https://ipil.lu/en/epo-a-study-on-inventorship-in-inventions-involving-ai-activity/> 4 November 2022.

[97] ibid; Ryan Abbott, 'I Think, Therefore I Invent: Creative Computers and the Future of Patent Law' (2016) 57 BCL Rev 1079, 1095.

[98] European Patent Office, 'EPO Publishes Grounds for Its Decision to Refuse Two Patent Applications Naming a Machine as Inventor' (28 January 2020) <www.epo.org/news-events/news/2020/20200128.html>; United States Patent and Trademark Office, 'Petition Decision – In Re Appl No 16/524,350 ('DABUS') (Inventorship Limited to Natural Persons)' (29 July 2019) <www.uspto.gov/sites/default/files/documents/16524350_22apr2020.pdf> both accessed 4 November 2022.

[99] Shemtov (n 96) 11.

[100] Although this is not always the case, see Filipe Maia Alexandre, 'The Legal Status of Artificially Intelligent Robots: Personhood, Taxation and Control' (17 June 2017) <https://papers.ssrn.com/abstract=2985466> accessed 4 November 2022.

[101] *Morse v Porter*, Bd Pat Inter (1965) 155 USPQ 280, 283.

[102] The Patents Act (UK) (1977) s 7(3).

For copyright, the relevant factor is the extent of human intervention in assisting or directing the AI to create the work. For example, the US Copyright Act of 1976 requires that a work has to be 'created by a human being',[103] the Canadian Copyright Act provides that an author must be a 'citizen or subject, or a person ordinarily resident',[104] and the Australian Copyright Act 1968 refers to a 'qualified person'.[105] Human intellectual authorship is a consistent precondition of copyright protection.[106]

As with patents, ownership of the copyright of AI outputs is the relevant question for investment protection. The UK Copyright, Designs and Patents Act 1988 specifically allows for the authorship of computer-generated works.[107] It provides that ownership vests in 'the person by whom the arrangements necessary for the creation of the work are undertaken'.[108] This person would be the covered investor. No such provision for computer-generated works exists in the Australian system.[109] Therefore, AI-generated works would not be capable of being subject to an IPR, and thus not protected as a copyright by an Australian investment treaty.

In general, the output of AI systems is capable of being protected as an IPR and thus would be a protected investment in IIAs. The current frameworks require that a human is involved in the invention or creation of the output and that a human or company gains ownership of these rights.

3.3 *The Uncertain Status of Data*

Unlike IPRs, investment treaties make no reference to data within the definition of investment. A difficult question in classifying data is whether related rights should be conceptualized as the right of ownership, right to benefit, or right of access.[110] Data is not subject to ownership in the European Union or the United States, but the storage and use of data in these jurisdictions remain subject to privacy and data protection regulations.[111] Therefore, there is a legal

[103] The term 'author' is not defined in the Act, but has been held to require a human creator, see *Naruto v Slater*, Case No 15-cv-04324-WHO (ND Cal) (27 January 2016).

[104] Copyright Act (Canada) (1985) RSC 1985 c C-42, s 5.

[105] Copyright Act (Australia) (1968) s 32.

[106] Jani Ihalainen, 'Computer Creativity: Artificial Intelligence and Copyright' (2018) 13 JIPLP 724.

[107] Copyright, Designs and Patents Act (UK) (1988) s 178.

[108] ibid 9(3).

[109] Ihalainen (n 106) 726.

[110] Teresa Scassa, 'Data Ownership' (11 October 2018) CIGI Papers No 187.

[111] Grace Park, 'The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act' (2020) 10 UC Irvine Law Review 1455.

nexus between data and its 'controller' that imposes certain rights and obligations, but the precise nature of this relationship is disputed.

Fortunately, these complex issues are not directly relevant for ascertaining whether data is protected within international investment law. To meet the jurisdictional requirements of arbitration, the relevant question is whether data falls within the definition of investment. While no arbitral cases have directly addressed the issue, two recent analyses have been conducted concerning the definition of investment within IIAs. One found that the threshold requirements of investment were 'complicated by likely met'[112] and the other that 'it is unlikely that data, whether in "raw" or processed form, would qualify as an "investment"'.[113]

As a starting point, IIAs have not expressly referenced data as a form of investment. Therefore, tribunals would have recourse to considering whether data qualifies as 'any kind of asset'. The accompanying list of covered investments is usually non-exhaustive and open-ended. A distinction should be drawn between unprocessed or 'raw' data, and data that has been processed in some way. IPRs expressly do not attach to the former, as they are not the product of intellectual effort nor do they have any degree of originality. An example of the latter would be 'database rights' in the European Union.[114] One method of including data within 'investment' would be to characterize access to an unprocessed dataset as an IPR. In the absence of any creative process, the only possible classification would be as a trade secret, which would require measures to be taken to protect the secrecy of the information, which represents a company's 'intellectual capital'.[115] As trade secrets (by definition) do not need to be registered to be an IPR, whether or not data-related 'secrets' would be classified as such is dependent on the applicable domestic law rules.

To qualify as an 'investment' under the ICSID Convention, there are additional criteria that must be satisfied. Commonly referred to as the 'Salini criteria', these involve the a contribution of money or assets, an assumption of risk, a certain duration, and a contribution to economic development.[116] Horvath and Klinkmuller have argued that data fails to satisfy these characteristics as

[112] Horváth and Klinkmüller (n 82) 608.

[113] 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.

[114] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases (27 March 1996) OJ L 77/20, art 1(2).

[115] EU Trade Secrets (n 92) art 1.

[116] *Salini Costruttori SpA and Italstrade SpA v Morocco* [*I*], ICSID Case No ARB/00/4, Decision on Jurisdiction (31 July 2001) [2003] 42 ILM 609, 52.

‘there is no “risk” in data’, ‘conceptualizing “data” in the context of duration makes little sense’ and ‘reams of “raw” data … contribute nothing to the economic development’.[117] Conversely, Mitchell and Hepburn contend that ‘given the generally expansive statements by tribunals, the ICSID requirements for an investment might ultimately be readily fulfilled even by investors in businesses relying heavily on cross-border data transfer’.[118]

The test of ‘every kind of asset’ sets a notably low jurisdictional threshold. ‘Investment’ is a broader concept than ‘property’. This is especially apparent in the absence of the more substantive analysis required by the International Centre for Settlement of Investment Disputes (ICSID) convention. While the more restrictive approach is undoubtedly correct about data being absent certain characteristics of investment activity, not all of these criteria must be satisfied in some instances.[119] Furthermore, ICSID tribunals have taken a permissive approach to jurisdiction for State owned enterprises, even though the preamble to the Convention mentions the promotion of ‘private investment’ and State-State claims are barred,[120] and intellectual property, even where it is not explicitly included in the definition of investment.[121]

One additional point might be made about the discrepancy between multinational companies’ ability to monetize data on the one hand, and the failure to ascribe adequate value to this data on the other. Excluding data from a definition as broad as ‘every kind of asset’ perpetuates this inability to reflect economic reality. As data-intensive industries become more prevalent, the classification of data within domestic economies, either as a property right or as an IPR, may have a knock-on effect on investment arbitration, though this is necessarily speculative. In any case, the specific circumstances of a claimant business relying on cross-border data flows may lead to a positive determination as to the existence of an investment.

[117] Horváth and Klinkmüller (n 82) 609.

[118] Mitchell and Hepburn (n 113) 218.

[119] One Tribunal found that the ‘criterion may not always be decisive’, *Malaysian Historical Salvors v The Malaysia*, ICSID Case No ARB/05/10, Award on Jurisdiction (17 May 2007) 108.

[120] Mark Feldman, ‘State-Owned Enterprises as Claimants in International Investment Arbitration’ (2016) 31 ICSID Rev 24, 31–34.

[121] Flavia Marisi and Julien Chaisse, ‘Is Intellectual Property “Investment”? Formation, Evolution, and Transformation of the Intellectual Property Rights: Foreign Direct Investment Normative Relationship’ (2019) 34 Ohio St J Disp Resol 97.

4 The Interaction Between the Regulation of Artificial Intelligence and Investment Treaty Obligations

Four categories of AI regulation may constitute barriers to investment: limitations on market access, restrictions on data flows, automated decision-making, and algorithmic transparency. Substantive investment treaty obligations will impact these barriers in cross-cutting ways. Therefore, this section will examine how AI regulations will interact with market access provisions, non-discrimination treatment, fair and equitable treatment, indirect expropriation, and the prohibition of performance requirements.

4.1 *Limits on Market Access and Enhanced Screening: A Limited Role for International Investment Agreements*

For reasons of privacy, security, or protectionism, States might respond to AI by restricting access to certain sectors or enhancing the screening of investors in high-tech sectors.

A State has the absolute right to prohibit, impose conditions, or allow the entry of aliens to its territory as a matter of general international law.[122] Positive rights of admission and establishment for foreign investment only arise by way of derogations to general international law through international treaties. A minority of IIAs do provide for such a derogation at the pre-establishment phase of an investment. These remain subject to sectoral or public policy carve-outs, some of which will exclude AI investments from protection.

However, non-discrimination provisions apply only to investors in the host State territory in the vast majority of IIAs. If States decide to restrict access to AI sectors, or block the acquisition of the technology companies on protectionist grounds, investment treaties will rarely be a vehicle for redress.

4.2 *Data Restrictions, Algorithmic Transparency, and Purpose-Based Non-Discrimination*

In the post-establishment phase, investors may seek to challenge the regulation of AI as a breach of the principle of non-discrimination. This typically requires States 'to accord to investors of another Party treatment no less favorable than that it accords, in like circumstances, to its own investors'.[123] In evaluating whether data restrictions or mandated algorithmic transparency will

[122] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 87.

[123] ibid 198.

constitute a breach, the first question is how to interpret the meaning of 'in like circumstances' to find an appropriate comparator.[124]

Attempts to develop a normatively justifiable set of criteria for 'in like circumstances' in abstract are doomed to fail, as '[b]y their very nature, "circumstances" are context-dependent and have no unalterable meaning across the spectrum of fact situations'.[125] Nevertheless, some tribunals have interpreted this to require comparison with a domestic investor with whom the claimant has a 'competitive relationship'.[126] Evidence in favor of the 'competitive relationship' test can be deduced from the preamble or stated objectives of IIAs, several of which include goals 'to promote competition'[127] and 'enhance competitiveness'.[128] In the context of the NAFTA, application of the competitive relationship test is justified by a clarification of the 1976 Organization for Economic Co-operation and Development (OECD) National Treatment Instrument, which provided that the applicable comparator was 'firms operating in the same sector'.[129] The Tribunal in *SD Myers* adopted a broad interpretation of the sector-based approach, and one of the determining factors was whether the claimant investor was 'in a position to attract customers that might otherwise have gone to Canadian operators'.[130]

For claims involving AI investment, the question is whether the appropriate comparator is a domestic firm that provides the same goods and services or a domestic firm that also utilizes AI. As the applicable test is one of 'competitive relationship', the appropriate comparator is surely the former. A foreign pharmaceutical company that utilizes AI as part of its research should be compared to other pharmaceutical companies. Non-discrimination provisions apply to the equality of opportunity concerning the good or service being produced, not the technology used in its production.

The second issue is what constitutes 'treatment less favorable'. In this respect, it is useful to distinguish between *de facto* and *de jure* 'treatment less

[124] Guiguo Wang, 'Likeness and Less Favourable Treatment in Investment Arbitration' (2016) 3 JICL 73, 75.

[125] *Pope & Talbot Inc v The Government of Canada*, NAFTA/UNCITRAL, Award on Merits Phase 2 (10 April 2001) 75.

[126] *SD Myers Inc v Government of Canada*, UNCITRAL, First Partial Award (13 November 2000) 251; *Pope & Talbot* (n 125) para 78.

[127] EFTA–Ecuador Comprehensive Economic Partnership Agreement (signed 25 June 2018, entered into force 1 November 2020) (CEPA) art 1.1.

[128] Korea–Viet Nam FTA (2015) preamble.

[129] The OECD National Treatment Instrument forms part of the OECD Declaration on International Investment and Multinational Enterprises (1976).

[130] *SD Myers* (n 126) para 251.

favorable'.[131] The relationship between the *de facto* and *de jure* depends on whether the applicable legal test of a measure is one of disparate impact or purposeful protectionism. If it is the former, then the threshold to breach the standard would be met if a regulatory measure had the effect of disadvantaging a foreign investor, even if this disadvantage was incidental to the aim of the measure. In *Siemans v Argentina*, the Tribunal adopted this approach in concluding that 'the impact of the measure on the investment would be the determining factor' when assessing a potential breach and 'intent is not decisive or essential for a finding of discrimination'.[132]

Data restrictions and algorithmic transparency may breach national treatment obligations. Let us return to the example of the foreign pharmaceutical company that utilizes AI. If only foreign investors in the pharmaceutical industry utilize AI technology, then mandating transparency of AI algorithms will negatively impact the foreign investors, but not domestic investors. If only the effect of the measure is relevant, such regulation would breach the standard, even if they were enacted for the protection of public health or public safety.

Numerous scholars have highlighted the flaws inherent in this disparate impact test.[133] It places an onerous burden on host States not to take measures that have a coincidental effect of disadvantaging foreign investors, even for a legitimate regulatory purpose.

A more persuasive approach is one that incorporates a purpose-based test of a State's regulatory measure. The guidance to the OECD National Treatment instrument provides support for this position. It stated that the central test 'is to ascertain whether the discrimination is motivated, at least in part, by the fact that the enterprises concerned are under foreign control'.[134] In *Pope & Talbot*, the Tribunal relied on this instrument in ruling that a measure will not breach the standard where it 'bears a reasonable relationship to rational policies'.[135] Focusing on intent has the tripartite benefit of respecting the State's capacity to make its own regulatory choices, creating a transparent doctrinal structure for the conditions for breach, and dissuading frivolous and speculative claims being by requiring a *prima facie* case of protectionist intent at

[131] Wang (n 124) 90.

[132] *Siemens AG v The Argentine Republic*, ICSID Case No ARB/02/8, Award (17 January 2007) 321.

[133] Jürgen Kurtz, *The WTO and International Investment Law: Converging Systems* (CUP 2016) 135.

[134] OECD Declaration on International Investment and Multinational Enterprises (n 129) 22.

[135] *Pope & Talbot* (n 125) para 79.

the outset.[136] There is some disagreement in respect of whether protectionist intent is the only criterion by which to assert a breach, or whether the measure must also be 'rationally connected to the least restrictive means of achieving a non-protectionist purpose'.[137] The latter approach considers protectionist purpose to be a prerequisite, but not sufficient, to finding a breach of national treatment.

Criticism of the purpose-only approach stems from difficulties inherent in proving intent. However, Kurtz has argued that the degree of disparate impact may be advanced as evidence of a constructive protectionist purpose.[138] By adopting this approach, the absence of overtly protectionist rhetoric would not prevent protectionist regulation being a breach of national treatment. Therefore, the 'constructive purpose' and 'least restrictive means' tests may prove to be overlapping, though not identical, analytical approaches in practice.

When the test is one of protectionist purpose, the imposition of data restrictions and algorithmic transparency will not breach standards of non-discrimination when it is for the protection of privacy, national security, or public safety. A disparate impact on AI investors will be insufficient to establish a breach. As these forms of AI regulation may be motivated by public policy and protectionism simultaneously, arbitrators may decide to apply a strict test that will find a violation where protectionism is a more-than-insignificant factor,[139] or a looser test where protectionism must be the dominant factor.[140]

In applying the least-restrictive-measure test, it is helpful to imagine a sliding scale. At one pole, the permissibility of cross-border data transfer is conditional on obtaining the consent of the data subject. At the other, investors are required to store, process, and access data locally, effectively prohibiting data transfer. The sensitivity of the data being transferred will likely determine whether a less restrictive measure could have obtained the same result.

Therefore, the interaction of disparate impact, protectionist purpose, and the least-restrictive measure tests will determine whether AI regulation

[136] Jürgen Kurtz, 'Balancing Investor Protection and Regulatory Freedom in International Investment Law: The Necessary, Complex, and Vital Search for State Purpose' in Andrea K Bjorklund (ed), *Yearbook on International Investment Law and Policy 2013–2014* (OUP 2015).

[137] Andrew D Mitchell, David Heaton and Caroline Henckels, *Non-Discrimination and the Role of Regulatory Purpose in International Trade and Investment Law* (Edward Elgar 2016).

[138] Kurtz (n 133) 174.

[139] Massimiliano Danusso and Ross Denton, 'Does the European Court of Justice Look for a Protectionist Motive Under Article 95?' (1990) 17 LIEI 67.

[140] Kurtz (n 136) 301.

complies with non-discrimination provisions. Conversely, compatibility with 'fairness' obligations will depend on the 'explainability' of the AI system and the context in which it is used.

4.3 *The (In)Compatibility of 'Black Box' Automated Decision-Making and Fair and Equitable Treatment*

The use of AI as part of decision-making processes will affect foreign investors in two ways: 'automated' governance decisions affecting their investments, and the activities of foreign investors that involve automated decision-making. Both are relevant for assessing host State compliance with the standard of fair and equitable treatment (FET).

Much like national treatment, a uniform understanding of the normative content of FET has proven elusive. This is perhaps inevitable given the inherent ambiguity of the terms 'fairness' and 'equity'. As arbitrators tend to interpret a series of arbitral cases as persuasive rather than strictly according to precedent, a limited convergence has begun to emerge for common principles of FET.[141]

These principles include due process and transparency. A denial of justice will occur where there is a 'manifest failure of natural justice in judicial proceedings or a complete lack of transparency and candor in administrative process'.[142] In *Thunderbird v Mexico*, the Tribunal undertook an analysis of an administrative proceeding in which it noted that the claimant 'was given a full opportunity to be heard and to present evidence', and found the subsequent administrative order 'to be adequately detailed and reasoned; it reviews the evidence presented by Thunderbird at the hearing; and discusses at length the legal grounds on which the Mexican Secretariat for Home Affairs (SEGOB) based its determination'.[143] The use of the term 'adequately' is indicative of a qualitative assessment of the reasoning. Furthermore, the Tribunal in *Lemire v. Ukraine* concluded that the awarding of licenses breached FET as it was 'without transparency, with total disregard of the process of law and without any possibility of judicial review'.[144] Due process and reasoned decision-making are established standards within investment jurisprudence.

[141] Kenneth J Vandevelde, 'A Unified Theory of Fair and Equitable Treatment' (2010) 43 NYU J Intl Law & Pol 43.

[142] *Waste Management v United Mexican States (II)*, ICSID Case No ARB(AF)/00/3, Award (30 April 2004) 98.

[143] *International Thunderbird Gaming Corporation v The United Mexican States*, UNCITRAL/NAFTA, Arbitral Award (26 January 2006) 198.

[144] *Joseph Charles Lemire v Ukraine (II)*, ICSID Case No ARB/06/18, Decision on Jurisdiction and Liability (14 January 2010) 418.

4.3.1 Algorithmic Governance Decisions Affecting Foreign Investors

Automated decisions that affect foreign investors will fall short of FET requirements if their processes do not meet these standards. In this regard, AI systems have a 'legal black box' problem and a 'technical black box' problem.[145] The former relates to the confidentiality afforded to proprietary information. Should a decision-making body decide that explaining the processes by which the decision was reached would comprise this propriety information, the individual affected by the decision may not be provided with written reasons.

The technical 'black box' problem is that the 'nature of AI techniques is characterized by an inherent lack of transparency, as decisional rules emerge automatically in ways that no one – even the programmers – can adequately explain'.[146] British philosopher Gilbert Ryle's distinction between 'knowing that' and 'knowing how' helps to explain the phenomenon.[147] The archetypal example is that of a child learning to ride a bicycle; providing a manual is unlikely to be helpful, nor will the child be able to explain a step-by-step approach to bike-riding once they are able to ride it successfully. After a process of trial and error, they just intuitively 'know how'.[148]

In the context of due process, the implications of this phenomenon are problematic. Even if the AI system is not limited by confidentiality requirements, the decision-making body may be unable to explain how the decision was reached, as they are not unable to fully understand the AI. The input data is processed in a 'black box' that is simply incongruent with a comprehensive right to reasons.

A case in point is the facts of *State v Loomis* in the United States.[149] An AI system – the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) – was used to predict the likelihood of reoffending.[150] Eric Loomis was adjudged by COMPAS to be at a 'high risk of recidivism' and was 'high risk to the community'. He was sentenced accordingly.[151] In seeking post-conviction relief, Loomis argued that the system violated his constitutional due process rights for three reasons: trade secrets prevented disclosure

[145] Yavar Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018) 31 Harv J L & Tech 890; Liu, Lin and Chen (n 5) 134.

[146] ibid 135.

[147] Gilbert Ryle, 'Knowing How and Knowing That: The Presidential Address' (1945) 46 Proceedings of the Aristotelian Society 1.

[148] Siddhartha Mukherjee, 'AI Versus MD: What Happens When Diagnosis Is Automated?' (*The New Yorker*, 27 March 2017) <www.newyorker.com/magazine/2017/04/03/ai-versus-md> accessed 4 November 2022.

[149] *State v Loomis*, State of Wisconsin Supreme Court (US) (2016) 881 NW 2d 749.

[150] ibid 754.

[151] ibid 755.

of the input data on which the decision was based, group data used to inform the algorithm violated the right to individualized sentencing, and the system improperly utilized gender-based assessment.[152] The Wisconsin Supreme Court rejected these claims.

Despite this ruling, which has been subject to some criticism, several features of the case may constitute a process that 'offends judicial propriety', notwithstanding the high threshold test in investment arbitration.[153] COMPAS was found to be 'remarkably unreliable', and 'only 20 percent of the people predicted to commit violent crimes actually went on to do so'.[154] No indication was given of the relative weighting afforded to specific criteria. Consequently, there was no opportunity to be heard on the evidence, no reasons given for the decision, and no transparency of the system. These are established features of FET. As such, automated decision-making may result in a breach of the standard.

Another principle of FET that does not sit comfortably with AI is the doctrine of legitimate expectations. The actions or legal environment of a State may create legitimate expectations for foreign investors which, if violated, would constitute a breach of FET.[155]

A possible conflict arises when governmental decisions are being made by an AI system, but the investors' expectations are created by humans. Human-centered governmental decision-making is burdened by the unconscious bias of conventional wisdom and by time and resourcing constraints.[156] Conversely, AI systems test for approaches that humans may have dismissed or not even considered, and can quickly process thousands of data points. Decisions by AI systems are, by their nature, creative and unforeseeable.[157] That foreseeability problem does not sit comfortably alongside specific commitments made to investors, nor expectations of a stable legal environment. The likelihood of this resulting in a breach of legitimate expectations will depend on the specificity of the relevant government commitment and

[152] ibid 757 and 760–67.

[153] Katherine Freeman, 'Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in *State v Loomis*' (2016) 18 North Carolina Journal of Law & Technology 75.

[154] Julia Angwin and others, 'Machine Bias' (*ProPublica*, 23 May 2016) <www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing?token=Gg58888u2U5db3W3CsuKrDoLD_VQJReQ> accessed 4 November 2022.

[155] Michele Potestà, 'Legitimate Expectations in Investment Treaty Law: Understanding the Roots and the Limits of a Controversial Concept' (2013) 28 ICSID Rev 88.

[156] Scherer (n 13) 364.

[157] ibid.

the extent to which the AI system is embedded within the decision-making process.

States' automated decisions may also breach FET if they involve discrimination or racial prejudice. The Tribunal in *Waste Management* considered that FET is infringed 'if the conduct is arbitrary, grossly unfair, unjust or idiosyncratic, is discriminatory and exposes the claimant to sectional or racial prejudice'.[158] The *Cargill* award concurred, considering that the customary minimum standard may 'relate to a lack of due process, discrimination, a lack of transparency, a denial of justice, or an unfair outcome'.[159]

4.3.2 Algorithmic Decision-Making by Foreign Investors

The problems of explainability and fairness can be equally important in the context of foreign investors that utilize AI. Whether investors who utilize AI can challenge AI legislation as a violation of the FET clause will depend on how each factual matrix interacts with established principles of FET. For example, the Tribunal in *Saluka* described the concept of an investor's legitimate expectations the 'dominant element' of FET. If a government official makes representations about the regulatory environment to attract high tech investors, failure to uphold specific commitments may give rise to a breach of IIAs. Readily identifiable obligations such as a contractual relationship may fall into this category,[160] but legitimate expectations may be created by informal representations, depending on the specificity of the representation.[161] Mere encouraging remarks to investors, or comments made in a political context will be likely be insufficient to meet the threshold. In *El Paso v Argentine Republic*, an investor attempted to reply upon a general statement by the President to the Congress as creating a legitimate expectation. The Tribunal held that 'a declaration made by the President of the Republic clearly must be viewed by everyone as a political statement, and this Tribunal is aware, as is every individual, of the limited confidence that can be given to such political statements in all countries of the world'.[162] Nevertheless, host States should be conscious of the legal consequences of comments and promises intended to induce investment in AI.

[158] *Waste Management* (n 142).

[159] *Cargill, Incorporated v United Mexican States*, ICSID Case No ARB(AF)/05/2, Award (18 September 2009) 285.

[160] *Glamis Gold Ltd v USA*, UNCITRAL/NAFTA, Award (8 June 2009) para 766.

[161] *Thunderbird Gaming Corp v Mexico* (n 143) para 147.

[162] *El Paso Energy International Company Claimant v the Argentine Republic*, ICSID Case No Arb/03/15, Award (31 October 2011) para 395.

Given the early stage of development of the AI sector and AI regulation, it is unlikely that investors would be successful in claiming that measures such as the DSA or AAA constitute a violation of their legitimate expectations in the absence of specific commitments.

Another route by which investors may seek to challenge AI regulation under FET is to claim that they are disproportionate to the goal being pursued. Proportionality and reasonableness are established principles of FET.[163] Tribunals have referred to a process of 'weighing' claimant and respondent interests. Of particular interest in the AI context are applications of the proportionality test that require considering whether a less restrictive measure may have been available. This was the case in *SD Myers*, in which the existence of less restrictive alternative measures was sufficient to establish a breach of NAFTA Article 1103.[164] Despite facing very similar circumstances, the EU has opted to regulate algorithmic decision-making to a greater degree than required by the United States. It would be for an arbitral tribunal to broach the high technical and value-laden question of whether there are sufficient differences in the respective policy goals to justify the more restrictive approach.

In this regard, arbitral tribunals have been inclined to balance claimant conduct against fairness obligations in assessing claims for breach.[165] In *Genin v Estonia*, the Tribunal held that revocation of a banking license 'must be considered in its proper context', part of which was a refusal to disclose the beneficial ownership of the parent company to financial regulators.[166] Failing to act with transparency and candor with regulatory authorities may be balanced against alleged violative conduct by host States. Therefore, if foreign investors that utilize AI as part of their service provision fail to act transparently in assessing issues of accuracy or discrimination, tribunals are likely to accord host States more latitude in requiring them to do so. Given that obligations for transparency stem from good faith principles, arbitrators may make a distinction between circumstances in which the AI investor has refused to comply and circumstances in which the AI investor has been unable to comply, with

[163] While these concepts are quite distinct in traditional public law, investment tribunals do not appear to make a clear distinction, see Marc Jacob and Stephan W Schill, 'Fair and Equitable Treatment: Content, Practice and Method' in Marc Bungen and others (eds), *International Investment Law: Handbook* (CH Beck, Hart, Nomos 2015).

[164] *SD Myers* (n 130) para 255.

[165] Peter Muchlinski, '"Caveat Investor"? The Relevance of the Conduct of the Investor Under the Fair and Equitable Treatment Standard' (2006) 55 ICLQ 527.

[166] *Alex Genin, Eastern Credit Limited, Inc and AS Baltoil v Estonia*, ICSID Case No ARB/99/2, Award (25 June 2001) 361.

the latter being viewed more favorably than the former. This might be the case for particularly advanced AI that use neural networks.

4.4 *Indirect Expropriation and the Differential Impacts of Artificial Intelligence Regulation*

Challenges to AI regulation are likely to involve the argument that such measures constitute a compensable indirect expropriation. The central issue is the threshold at which government interference moves from a non-compensable regulatory measure to indirect, compensable expropriation. Methodological approaches to this question can be divided into the 'sole effects' test, the 'police powers' test, and the proportionality test, with the second and third occasionally overlapping. Each approach has a different consequence for AI investors.

The sole effects test is one that considers the effect of the measure as the primary focus of inquiry, with a restricted role for an intention to expropriate. The Tribunal in *Vivendi v Argentina* (*II*) considered that the inquiry is 'directed particularly at the "effects" of the measure on the investment, rather than at the intent of the government enacting the measure'.[167] In general, tribunals have adopted a standard of 'substantial deprivation'.[168]

The requirement that data be held on local servers would likely be an inconvenience for businesses that rely on cross border data transfer, but it is difficult to conceive of a circumstance in which this would result make ownership rights 'practically useless'.[169] Businesses are likely to adapt. One example is file hosting service Dropbox, that has taken steps to store their data locally to comply with GDPR provisions.[170] Consequently, it is unlikely that data localization measures would constitute an indirect expropriation.

For algorithmic transparency, AI investors are susceptible to 'substantial deprivation' because of the extent to which their economic value is bound up in intellectual property. In the absence of confidentiality rules to prevent the dissemination of trade secrets, administrative processes that require the

[167] *Vivendi v Argentina* (*II*), ICSID Case No ARB/03/19, Decision on Liability (30 July 2010) 133.

[168] *Pope & Talbot v Canada*, UNCITRAL, Interim Award on Merits (26 June 2000) 102; *Metalclad Corporation v Mexico*, ICSID Case No ARB(AF)/97/1, Award (30 August 2000) 103; *CMS Gas Transmission Company v Argentina*, ICSID Case No ARB/01/8, Award (12 May 2005) 262.

[169] *Compañia del Desarrollo de Santa Elena SA v Costa Rica*, ICSID Case No ARB/96/1, Award (17 February 2000) 78.

[170] Thomas Hansen, 'Dropbox Is Growing in Europe' (*Dropbox Business Blog*, 11 February 2016) <https://blog.dropbox.com/topics/company/dropbox-is-growing-in-europe> accessed 4 November 2022, cited in Mitchell and Hepburn (n 113).

disclosure of algorithms could lead to a severe diminution in the value of the business.

If intent is not a relevant factor, measures motivated by protectionism that target AI investors will be subject to the same test as other regulatory measures. Protectionist measures are defined by their intent. However, it seems likely that the (post-establishment) imposition of market access restrictions would meet the 'substantial deprivation' standard, as the investor would be deprived of any meaningful use of the property.

The second approach taken by tribunals is the 'police powers' test, which is characterized by an evaluation of the broader purpose and context of the measure.[171] In *Philip Morris v Uruguay*, the Tribunal stated that a 'bona fide exercise of police powers in such matters as the maintenance of public order, health or morality, excludes compensation even when it causes economic damage to an investor'.[172] A similar approach was taken in *Methanex v United States*, in which it was held that 'a non-discriminatory regulation for a public purpose' would not be expropriatory in the absence of specific commitments by the government to an investor.[173] Considerations of reasonableness or proportionality were not relevant.

Given the safety concerns raised by autonomous vehicles and the various defense-related applications of AI, it is plausible that States will argue that related regulatory measures should be considered non-compensable. National security and the protection of human life are certainly public purposes. While the status of privacy is less established, the growth in cross-border data flows and frequency of data collection activities has elevated data protection to new prominence as a distinct area of public policy. Whether measures were 'taken for' these public purposes will be highly dependent on the circumstances.

The third approach is a test of proportionality, which can be a component of the police powers test.[174] *Tecmed v Mexico* is commonly quoted for the proportionality test, in which the Tribunal stated 'there must be a reasonable relationship of proportionality between the charge or weight imposed to the foreign investor and the aim sought to be realized by any expropriatory measure'.[175]

The first stage of analysis would be relatively straightforward to satisfy for AI regulation. It requires merely the identification of a threat to security, privacy,

[171] Dolzer and Schreuer (n 122) 120.

[172] *Philip Morris Brands* (n 79) para 295.

[173] *Methanex Corporation v United States of America*, UNCITRAL, Final Award of the Tribunal on Jurisdiction and Merits (3 August 2005) 278.

[174] Dolzer and Schreuer (n 122) 123.

[175] *Técnicas Medioambientales Tecmed v Mexico*, ICSID Case No ARB(AF)/00/2, Award (29 May 2003) 115, para 122.

or public safety and that data restrictions and algorithmic transparency are directed towards them.

The second stage of analysis is to consider whether the measure was 'necessary' and the 'least-restrictive measure', which has a higher threshold. In a circumstance where an autonomous vehicle has been involved in a collision, it may be necessary to require the disclosure of the intellectual property controlling the vehicle involved in that collision. However, it may not be regarded as the least restrictive measure to require the publication of the internal algorithms of all autonomous vehicles on a public registry. Similarly, the effectiveness of data localization to achieve objectives related to security or privacy is a highly technical matter.[176] Given the relative infancy of AI technologies, there is little practice by which to judge whether a measure is necessary, and even less practice on whether it was the least restrictive measure available to regulators.

The third stage of analysis – weighing the impact of the measure on the investor against the aim being pursued – involves weighing values that are vague and unsettled. How should privacy be balanced against innovation? How should public safety be ensured when regulating autonomous vehicles? These are questions to which many legal jurisdictions do not yet have answers. As such, any weighing and balancing undertaken by arbitrators is bound to be unpredictable.

4.5 *Technology Transfer and Data Localization as Performance Requirements*

A limited number of IIAs prohibit the imposition of performance requirements.[177] Common performance requirements are minimum requirements for local equity, local employment, local content, conducting research within the host territory, pursuing specific economic or social policies, or transferring technology.[178]

Legislation mandating that investors store data locally may constitute a prohibited local content requirement. The Canada-Senegal BIT provides that a party must not impose a requirement, commitment or undertaking 'to achieve a given level or percentage of domestic content' or to 'to purchase, use or accord a preference to a good produced or service provided in its territory, or

[176] Anupam Chander and Uyên Lê, 'Data Nationalism' (2015) 64 Emory L J 677.

[177] See generally Alexandre Genest, *Performance Requirement Prohibitions in International Investment Law* (Brill Nijhoff 2019) 52.

[178] ibid 139.

to purchase a good or service from a person in its territory'.[179] Depending on how the data localization measure is drafted, it could fall foul of either of these provisions. If a certain percentage of data must be stored locally, it constitutes the first; if the investor must use data servers located in the territory, or use specific servers to do so, it constitutes the second.

Furthermore, regulations mandating algorithmic transparency and technology transfer could violate prohibitions of performance requirements. NAFTA Article 1106 provides that no party can enforce obligations 'to transfer technology, a production process or other proprietary knowledge to a person in its territory'.[180] However, the prohibition is caveated by 'except when the requirement is imposed or the commitment or undertaking is enforced by a court, administrative tribunal or competition authority to remedy an alleged violation of competition laws'.[181] It also excludes a 'measure that requires an investment to use technology to meet generally applicable health, safety or environmental requirements' from the prohibition on technology transfer.[182]

Given the broad formulation of 'technology, production process or other proprietary knowledge', the intellectual and intangible property of AI benefits from protection. Qin has highlighted that technology transfer generally takes two forms: the disclosure of proprietary information in an administrative process and the ownership rules for permitting the entry of foreign investors.[183] Ownership rules constitute market access restrictions, and so would not fall foul of investment treaty obligations that are limited to the post-establishment phase of an investment.

Disclosure of source code or algorithms as part of administrative processes will become a necessary accompaniment of its use in certain contexts. The more difficult question is how to apply the provision when the administrative tribunal or process is the means by which to force the technology transfer. It is a common complaint of the United States that the administrative processes for gaining market access in China involve the disclosure of proprietary information and trade secrets that are not germane to genuine regulatory concern.[184] Going further, it has been alleged that this information has been provided to domestic competitors, though this is specifically prohibited under China's new

[179] Canada–Senegal BIT (2014) art 9(1).

[180] North American Free Trade Agreement Between Canada, Mexico, and the United States (17 December 1992, entered into force 1 January 1994) (NAFTA) art 1106(1)(f).

[181] ibid.

[182] ibid art 1106(2).

[183] Qin (n 55) 744.

[184] ibid 743.

Foreign Investment Law.[185] Even if disclosure is required as part of an administrative tribunal, the alleged practice will breach prohibitions on technology transfer that refer to TRIPS which provides that data provided by governmental agencies is protected from unfair commercial use.[186]

5 The Inadequacy of Existing Defenses for Artificial Intelligence Investment

Given the investment and trade barriers that AI systems will provoke, the scope and content of exceptions clauses are crucial to establish the extent to which measures affecting this emerging technology will comply with international obligations. As a preliminary matter, the vast majority of IIAs do not contain exceptions. Most respondent States would be reliant on arbitrators to reengineer questions of public policy as part of investment obligations. For those IIAs that do include general exceptions clauses, there are often conditions for its invocation, including that the measure must not be 'a disguised restriction on investors'. Under such provisions, States would be unable to rely on exceptions to shield overtly protectionist measures.

For the regulation of AI, two problems arise: the narrow drafting or interpretation of permissible objectives, and the highly technical questions raised by the requirement that a measure is 'necessary'.

5.1 *Narrow Drafting Is Not Inclusive of Relevant Security and Privacy Concerns*

A common formulation of security-related exceptions is that of 'essential security interests', but other security-related terms include 'national security', 'public order', 'international peace or security', 'circumstances of extreme emergency', and 'measures related to the production, trade and development of arms and other defense material'. Each of these formulations has a potentially different impact on a regulatory measure.

[185] Article 22 of the Foreign Investment Law of the People's Republic of China (adopted 15 March 2019, entered into force 1 January 2020) provides that 'Administrative organs and their employees must not force the transfer of technology through administrative measures'.

[186] The Agreement on Trade-Related Aspects of Intellectual Property Rights (signed 15 April 1994, entered into force 1 January 1995) (TRIPS Agreement) art 39.

Some commentators have argued for a restrictive interpretation of 'essential security interests' that limits its application only to militaristic activities.[187] Indeed, the International Court of Justice (ICJ) in the *Nicaragua Judgment* (*Merits*) narrowly interpreted 'essential security interests' in rejecting the defense that 'the policies and actions of the Government of Nicaragua constitute an unusual and extraordinary threat to the national security and foreign policy of the United States'.[188] Adopting this restrictive approach, the use of AI as part of military technologies or to support armed attack would fall within its definition, but utilizing AI to foment political turmoil would not. Even if a tribunal was to take a broader reading of the phrase, such as in *LG&E v Argentine Republic*, the circumstances in which 'the severity of the problem can equal that of any military invasion' is likely to be very limited for AI.[189]

Conversely, variations such as measures 'relating to the traffic in arms, ammunition, and implements of war' may encompass a wider array of interests.[190] A pertinent example is the aforementioned Project Maven, in which Google – a civilian company – was contracted to develop imagery analysis for weaponry. An interesting question is whether 'defense material' is interpreted to include instruments of cyber-defense, or whether it is limited to conventional weapons. If it is the former, the scope of this exception is expanded significantly and covers the uses of AI which could be utilized as a part of cyber-attacks.

The problem is that AI-driven asymmetric warfare clearly engages issues of 'national security' (broadly construed) and 'public order' if it is used as a tool to foment social unrest or promote radicalism. US BIT practice provides that 'public order' covers 'measures taken pursuant to a Party's police powers to ensure public health and safety', which seemingly includes measures taken by law-enforcement during peacetime.[191] However, most IIAs are absent any such clarification.

Turning to the issue of privacy, only a small minority of IIAs contains exceptions for non-security public policy issues. Commonly included permissible objectives are the protection of human, animal or plant life, public health, public morality, national or artistic treasures, and the conservation of

[187] William J Moon, 'Essential Security Interests in International Investment Agreements' (2012) 15 JIEL 481.

[188] *Nicaragua v United States of America* (Merits) [1986] ICJ Rep 14, 224.

[189] *LG&E Energy Corp, LG&E Capital Corp and LG&E International Inc v Argentine Republic*, ICSID Case No ARB/02/1, Decision on Liability (3 October 2006) para 238.

[190] NAFTA (n 180) art 1202(1)(b)(i).

[191] William W Burke-White and Andreas von Staden, 'Investment Protection in Extraordinary Times: The Interpretation and Application of Non-Precluded Measures Provisions in Bilateral Investment Treaties' (2008) 48(2) Va J Intl L 307.

exhaustible national resources. AI regulation applied in pursuit of these public policy areas would considered to be in pursuit of a permissible objective. For example, a requirement that health records must be stored locally may fall under the public health exception, even in the absence of an explicit exception for privacy.

Nevertheless, the treaty practice of a limited number of States – Singapore, Japan, Canada, and the European Union – reflect the emergence of privacy as a permissible objective within IIAs. The Japan-Armenia BIT refers to 'the protection of the privacy of the individual in relation to the processing and dissemination of personal data'.[192] While a rarity in the context of IIAs overall, the inclusion of privacy as an explicitly-stated permissible objective may prove to be an emerging trend as concerns around cross-border data transfer become more prominent. It is limited to those measures which are 'not inconsistent with the provisions' and so does not create a positive right. In such circumstances, data restrictions aimed at privacy will fall within the scope of the general exceptions clause if it is 'necessary'. This may prove to be a highly technical and value-laden question.

5.2 *The Technical and Value-Laden 'Necessary' Test in Artificial Intelligence Contexts*

To be excepted from substantive provisions, AI regulation must be 'necessary' to achieve a permissible objective.[193] Self-judging iterations of this nexus requirement may prove of limited utility for AI investors that are subjected to protectionist or disproportionate regulation.[194]

Non-self-judging clauses stipulate that a regulatory measure must be 'necessary' to achieve the public policy being pursued. The distinction between the 'necessary' test in IIAs and the 'necessity' test in the ILC Articles of State Responsibility has been the subject of considerable scholarly analysis and need not be discussed here.[195] It is sufficient for our purposes to acknowledge that the two tests should not be conflated, and the 'necessary' requirement is a separate standard.

In *Handyside v United Kingdom*, the European Court of Human Rights (ECtHR) considered that the adjective 'necessary' is not so restrictive as to

[192] Japan–Armenia BIT (2018) art 16(c)(ii).

[193] Prabhash Ranjan, '"Necessary" in Non-Precluded Measures Provisions in Bilateral Investment Treaties: The Indian Contribution' (2020) 67 NILR 473.

[194] The Tribunal in LG&E held good faith to be implicit. *LG&E Energy Corp* (n 189) para 214.

[195] August Reinisch, 'Necessity in International Investment Arbitration – An Unnecessary Split of Opinions in Recent ICSID Cases – Comments on *CMS v Argentina* and *LG&E v Argentina*' (2007) 8 JWIT 191.

require that the measure be 'indispensable', and not so flexible as to require that it merely be 'desirable'.[196] It sits between these poles, granting a 'margin of appreciation' to Contracting States but not an 'unlimited power of appreciation'.[197] The Court considered the test to be one of proportionality. Traditionally, three stages of analysis are embedded within the test of proportionality: a rational connection between the regulatory measure and policy objective, whether the objective can be achieved by less restrictive means, and 'balancing' whether the effect regulatory measure is disproportionate to the objective being pursued.[198] These steps incrementally heighten the threshold test, with the final stage permitting judges to weigh the relative value of competing interests. However, advocates of the proportionality approach in investment arbitration often do not envisage a three-step proportionality review outlined above, but instead, propose only the third 'balancing' stage.[199]

In the AI context, an assessment of proportionality presents a particular difficulty because of the absence of international norms governing its use. At the balancing stage, decisions of national legislators on complex, value-driven policy issues are therefore supplanted by the judgment of the adjudicator. This is problematic in traditional investment contexts and is even more so when the goals being balanced – privacy in this case – are so novel, inconsistently regulated, and fast-moving. For example, there is no international consensus for the legitimacy of digital surveillance. Unlike the European Union, the international investment regime is not tasked with a pursuit of a normative goal such as positive integration, nor is there an appellate mechanism to ensure this goal manifests in a coherent body of law.[200] As such, there is no 'guiding star' to support the legitimacy of a proportionality test in investment arbitration and certainly not in the context of the regulation of AI.

Alternatively, the Tribunal in *Continental Casualty* interpreted WTO jurisprudence in stating that the test was the least-restrictive measure that 'that would have yielded equivalent results/relief'.[201] This is a highly technical question in AI contexts. Innovation in AI is far outstripping the pace of regulatory structures, and arbitrators are simply not qualified to judge the relative

[196] *Handyside v United Kingdom*, App No 5493/72 (ECtHR, 4 November 1976) 48.

[197] ibid 49.

[198] Alec Stone Sweet and Jud Mathews, 'Proportionality Balancing and Global Constitutionalism' (2008) 47 Colum J Transnatl L 72, 74.

[199] Jürgen Kurtz, 'Adjudging the Exceptional at International Investment Law: Security, Public Order and Financial Crisis' (2010) 59 ICLQ 325, 367.

[200] ibid.

[201] *Continental Casualty Company v Argentine Republic*, ICSID Case No ARB/03/9, Award (5 September 2008) 198.

restrictiveness of measures by comparison to other State practices. Permitting expert testimony and interventions from relevant organizations will be an imperative of arbitrations involving AI investors. Indeed, this is part of a set of proposal to prepare international investment law for an AI-driven future.

6 Optimizing International Investment Law for an Artificial Intelligence-Driven Future: An Overview of Reformative Measures

Regulatory responses to the growing incidence of AI in the global economy may force arbitral tribunals to weigh a complex array of interests to assess potential violations. This article has argued that the international investment regime has a role to play in balancing these diverging interests, but that it can be an inconsistent and unpredictable legal environment to do so. Given that the primary function of early BITs is the furtherance of investment protection, such incoherence is perhaps unsurprising. However, three threads of reform can enhance consistency and optimize international investment law for AI-related disputes: (A) reinforcing the anti-protectionist purpose of investment treaties through institutional reform and more precise drafting; (B) incorporating standards on human-centric ethics norms for AI within investment treaties; and (C) clarifying provisions on amicus curiae briefs and expert evidence.

6.1 *Reinforcing the Anti-Protectionist Purpose of Investment Treaties*

The spread of adjudicatory choices makes it challenging to identify a consistent methodology for defining the limits of substantive obligations; few analytical approaches to national treatment, FET, expropriation, or exceptions are truly generalizable. This article has argued that a doctrinally justifiable approach is to allow respondent States to present the public interest justification against claims of breach. Going forward, the central question is how to encourage arbitrators to produce a coherent body of jurisprudence that builds commitment by investors and States.

One corrective method is structural reform. The test case is the European Union's Investment Court System, which establishes a permanent adjudicative body and an appellate mechanism. Members of the tribunal must have the same qualifications for the International Court Justice, not act as a counsel or party-appointed expert in any other case, be free from conflicts of interest, and adhere to a strict code of ethics.[202] Whether or not the institutionalization of

[202] Freya Baetens, 'The European Union's Proposed Investment Court System: Addressing Criticisms of Investor-State Arbitration While Raising New Challenges' (2016) 43 LIEI 367.

investment arbitration will be embraced by States remains an open question, but these reforms certainly remove the incentives of adjudicators to adopt interpretive methods for reasons unrelated to the dispute.

Aside from structural reform, States have begun to limit arbitral discretion by drafting investment obligations with greater precision.[203] Some modern IIAs clarify that the purpose of national treatment is to ensure that foreign investments are not treated less favorably on the basis of their nationality. Similarly, recent treaties contain an illustrative list of prohibited behaviors under FET and clarify its relationship to the international minimum standard. Expropriation clauses incorporate guidance as to the factors to be considered in determining the existence of indirect expropriation. By delineating the contours of these obligations more exactly, contracting parties secure appropriate regulatory space and enhance the stability and predictability of the regime.

6.2 *Embedding Human-Centric Ethical Principles for Artificial Intelligence*

While embedding policy considerations like privacy and security will contribute to resolving AI-related disputes, investment treaties do not contain extensive technical provisions for AI or data transfer. Nor is it necessarily appropriate that they do so. Coherent disciplines on AI regulation will emerge from external sources, such as international organizations, private stakeholders, and national regulators.

In May 2019, forty OECD member countries approved the OECD Council Recommendation on Artificial Intelligence that establishes principles for the responsible development of trustworthy AI.[204] The principles include: inclusive growth, sustainable development, and well-being; human-centered values and fairness; transparency and explainability; robustness, security and safety; and accountability.[205] Data is given particular attention in the recommendations for international cooperation, with an emphasis on the 'ethical sharing of data' and the promotion of 'consensus-driven global technical standards'.[206] In April 2019, the European Union's High-Level Expert Group on AI also presented Ethics Guidelines for Trustworthy Artificial Intelligence.[207] The

[203] Caroline Henckels, 'Protecting Regulatory Autonomy Through Greater Precision in Investment Treaties: The TPP, CETA, and TTIP' (2016) 19 JIEL 27.

[204] OECD Principles on Artificial Intelligence (adopted 22 May 2019).

[205] ibid 1.1–1.5.

[206] ibid 2.2, 2.5(c); 'G20 Ministerial Statement on Trade and Digital Economy' (8–9 June 2019) 11.

[207] European Commission, 'High-Level Expert Group on Artificial Intelligence' <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai> accessed 4 November 2022.

guidelines closely align with the OECD principles and emphasize human agency, data governance, and transparency.

From the perspective of investment law, the relevant inquiry is how these principles will help arbitrators delineate between legitimate public-interest regulation and violative protectionist measures. References to privacy, data protection, and the ethical sharing of data are a recognition that cross-border data transfer does engage matters of public policy. Arbitrators may consider privacy or human rights an ample justification for restrictions on cross-border data transfer. Moreover, stipulations that AI should be explainable and transparent will be relied upon by host States to justify mandating algorithmic transparency and may be relied upon by investors claiming unfair treatment. Indeed, the general focus upon 'human-centered' AI gives relatively broad latitude for governments seeking to regulate AI in the private sector and contributes towards the standards to be expected by investors in their treatment by AI-powered public sector bodies.

There should be two notes of caution. Firstly, these principles have been developed by intergovernmental institutions that are dominated by Western and developed nations. As such, they may not take account of the effect of AI on countries whose route to prosperity will be affected by the data-driven economy. In the case of data, there are emerging data realms that reflect the unique conditions of respective rule-makers; the Chinese regime focuses on security, the European regime on human rights, and the US regime on consumer rights. Each in their own way has attempted to export their approach through extraterritorial application or through international instruments. Might we see a similar phenomenon with AI? Could IIAs become an instrument through which to diffuse AI policy with trading partners? Certainly, the EU is not averse to linking human rights to trade policy in the Generalised Scheme of Preferences. Given this context, it seems plausible that adoption of EU AI standards would become a precondition for the trade of investment of AI technologies, with 'mutually agreed standards' becoming a feature of modern investment and trade agreements. Conversely, China's model of data sovereignty and use of AI as a surveillance tool may appear attractive to authoritarian regimes. Rather than characterizing emerging AI norms as 'convergence' or 'divergence', it may be better to consider nascent spheres of influence according to certain shared characteristics and how AI might be deployed.

Secondly, principles alone will be insufficient to develop detailed and unambiguous standards of data protection and algorithmic disclosure. Drawing a distinction with medical ethics, Mittelstadt has highlighted that the aims of the AI profession do not necessarily align with the public interest, there is no historically validated account of beneficial AI development, there are few proven methods to translate principles into practice, and no mechanisms of accountability or redress for a breach of ethics.[208] Consequently, the apparent consensus for AI principles is of limited value as 'translating principles into practice will remain a competitive, not cooperative, process'.[209]

Nevertheless, these human-centric ethical principles for AI can contribute to phases of investment law and arbitration. At the drafting phase, comments should be invited from international organizations and private initiatives on technical standards for data protection and algorithmic transparency. The technical community includes the Future of Life Institute; the Institute for Electrical and Electronics Engineers (IEEE); the Japanese Society for Artificial Intelligence; Fairness, Accountability, and Transparency in Machine Learning (FATML); and the Association for Computing Machinery, all of which are developing initiatives on ethical development of AI.[210]

In the future, governments should consult these stakeholders when drafting the provisions of BITs, data protection regulations, and technology transfer requirements to ensure that a balance is being struck between public interest regulation and liberalized investment policy. For older BITs, ethical principles can contribute to arbitral disputes over AI regulation through expert witness testimony and the submission of amicus curiae briefs.

6.3 *Provision for Expert Witnesses and* Amicus Curiae

To determine whether an AI regulation is the least restrictive measure available to host States, evidence is required on the viability of alternative measures, the different economic impact of these alternatives, and guidance as to the quantum of damages appropriate for data-intensive activities.

ICSID Arbitration Rules 34(2) and 35 explicitly provide for the admissibility and examination of expert evidence.[211] Article 27(2) of the 2010 United Nations Commission on International Trade Law (UNCITRAL) Arbitration Rules amended references to 'witnesses' in the 1976 Arbitration Rules to 'witnesses, including expert evidence'.[212] Parties are afforded the opportunity to express their opinion on the expert's report, interrogate the expert on their evidence, and present their own witnesses to testify on the relevant points.[213]

[208] Brent Mittelstadt, 'Principles Alone Cannot Guarantee Ethical AI' (2019) 1 Nature Machine Intelligence 501.

[209] ibid 505.

[210] For a selection of guidelines for AI developed by shareholders, see OECD, 'Artificial Intelligence in Society' (OECD, 2019) 123.

[211] ICSID Arbitration Rules (2006) arts 34(2) and 35.

[212] UNCITRAL Arbitration Rules (2010) art 27.

[213] ibid.

While recent iterations of both the ICSID Arbitration Rules and UNICITRAL Arbitration Rules provide that expert witnesses can contribute to arbitral proceedings, the rules are short on detail as to the form of the evidence and means of examination.[214]

Comparatively detailed rules on the admissibility, form, and examination of expert evidence are contained in the International Bar Association Rules on the Taking of Evidence in International Arbitration (the IBA Rules).[215] In light of the necessity of expert evidence for regulations affecting AI and the data-driven economy, more detailed provisions in the IBA Rules is welcome. The expert opinion, alongside a description of the methods and information on which it is based, must be provided to the tribunal in a written report 'as a means of evidence on specific issues'.[216] Fears that experts act as 'hired guns' have been addressed by provisions on ethical standards. These include transparency concerning instructions given by parties, a mandatory statement of independence, and affirmation of a genuine belief in the opinion being expressed.[217] Provision is also made for a tribunal to order party-appointed experts to 'reach agreement on the issues within the scope of their expert report' and provide a written account of issues on which they were and were not able to do so.[218]

In reviewing this regulatory landscape, two recommendations can be made to optimize the rules on expert witnesses for AI-related disputes. Firstly, the IBA Rules should be utilized to fill the procedural gaps in the ICSID Arbitration Rules and UNCITRAL Arbitration Rules. Secondly, tribunals should request some form of collaboration between multiple experts, either by requesting joint expert reports, permitting the simultaneous cross-examination of multiple experts through 'expert conferencing', or creating an 'expert team' comprised of one expert drawn from each party's list of potential experts.[219]

While neither expert reports nor amicus curiae briefs should constitute advocacy, the submissions of the latter generally come from non-governmental organizations with an interest in the outcome of proceedings. For regulatory measures affecting AI, third party submissions may be justified and necessary

[214] Brooks W Daly and Fiona Poon, '11 Technical and Legal Experts in International Investment Disputes' in Chiara Giorgetti (ed), *Litigating International Investment Disputes: A Practitioner's Guide* (Brill Nijhoff 2014) 326.

[215] International Bar Association (IBA) Rules on the Taking of Evidence in International Arbitration (2010).

[216] ibid art 5(1).

[217] ibid art 5(2)(b),(c),(g).

[218] ibid art 5(4).

[219] Daly and Poon (n 200) 332.

as the inherent human rights, privacy, and public safety concerns transcend the individual dispute.

As the acceptance of amicus curiae briefs has emerged as a feature of investment arbitrations, provisions for their submission have been incorporated in arbitration rules and investment treaties. Since 2006, Rule 37 of the ICSID Arbitration Rules has provided for submissions by non-disputing parties that would 'assist the Tribunal in the determination of a factual or legal issue related to the proceeding by bringing a perspective, particular knowledge or insight'.[220] A supplemental set of 'Rules on Transparency in Treaty-based Investor-State Arbitration' has also embedded third-person submissions within the UNCITRAL Arbitration Rules,[221] while the rules of the Arbitration Institution of the Stockholm Chamber of Commerce and Singapore International Arbitration Centre now accommodate amicus curiae submissions.[222] Consequently, even in the absence of specific treaty provisions allowing for such submissions, the procedural rules of arbitration institutions are permissive.

Given the privacy and human rights concerns inherent in AI technologies, it may be advisable that States directly provide for the admissibility of amicus curiae briefs within investment treaties. This can be achieved in two ways. The first is to incorporate the UNCITRAL Rules within BITs, such as in the EU-Canada Comprehensive Economic and Trade Agreement (CETA).[223] Secondly, contracting parties can embed distinct amicus provisions in the treaty, as is the case in the Trans-Pacific Partnership.[224]

7 Conclusion

Restrictions on data transfer, mandates for algorithmic transparency, automated decision-making, and limitations on market access are, to varying

[220] ICSID Arbitration Rules (2006) Rule 37(2)(a).

[221] UNCITRAL Rules on Transparency in Treaty-based Investor-State Arbitration (2014) art 4.

[222] Singapore International Arbitration Centre Investment Arbitration Rules (2016) art 29.2; Arbitration Rules of the Arbitration Institute of the Stockholm Chamber of Commerce (2017) Appendix III 'Investment Treaty Disputes', art 3.

[223] EU–Canada Comprehensive Economic and Trade Agreement (signed 30 October 2016, provisionally entered into force 21 September 2017) (CETA) art 8.38.

[224] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (signed 8 March 2018, entered into force 30 December 2018) (CPTPP) art 9.23.

degrees, barriers to foreign investment. In some instances, they are also rational regulatory responses to the public policy issues engaged by AI.

In seeking to explore the pivot points at which AI meets investment law, this article has argued that the international investment regime provides an unpredictable legal environment in which to adjudicate the emerging norms and ethics of AI. IIAs play a limited role in the pre-establishment phase of most investments; substantive protections apply only after the investment is established in the host State. It is difficult to identify representative lines of case law to elucidate the normative content of these protections, and the problems of foreseeability and explainability with AI present complications to complying with FET. Against the background of potential breaches of treaty standards, exceptions for public policy are comparatively rare in the global treaty network, and reference to standards of privacy are even rarer. As such, questions as to whether AI regulation is 'necessary' or the 'least restrictive measure' force arbitrators to make technical and value-laden judgements about contested principles.

Several reforms can mitigate the uncertainty. Treaty standards should be drafted with more precision to reinforce their anti-protectionist purpose. Human-centric AI principles can be embedded to balance privacy, safety and the demands of innovation. Tribunals should embrace expert witnesses and amicus briefs.

As the growth of the data-driven economy and artificial intelligence continues apace, investment treaties and investment arbitration must adapt to accommodate these new concerns – they are here for the long term.