13

# International Trade Law and Data Ethics

## *Possibilities and Challenges*

*Neha Mishra*

## I INTRODUCTION

The global economy is constantly being reshaped because of the rapid growth of data-driven services and technologies. The complementary relationship of big data analytics and artificial intelligence (AI)[1] holds the potential to generate significant economic and social benefits.[2] However, such data-driven services can also be misused by companies, governments and cyber-criminals in different ways, resulting in increased privacy and security breaches; disinformation campaigns; and biased algorithmic decision-making that disempower users of such technologies/services.[3] These misuses often result because of deficiencies/loopholes in how data-driven services collect, process, transfer and share data, as well as the technical design of their algorithms or computer programs, thereby raising strong concerns regarding the ethics of data management and data-driven technologies. In response to these concerns, several governments and private initiatives have formulated data ethics frameworks that regulate data-driven technologies.[4] Similarly, scholars have started evaluating how data ethics principles can act as a 'moral compass' in determining 'good' digital regulation and

[1] J Yeung, 'What Is Big Data and What Can Artificial Intelligence Do?' (Towards Data Science, 30 January 2020), perma.cc/Z7CS-JZQ3.

[2] T Philbeck et al., 'Values, Ethics and Innovation Rethinking Technological Development in the Fourth Industrial Revolution' (White Paper, World Economic Forum, August 2018), at 4; Organisation for Economic Co-operation and Development (OECD), 'Data-Driven Innovation for Growth and Well-Being' (2015), www.oecd.org/sti/ieconomy/data-driven-innovation.htm; World Health Organization, 'Big Data and Artificial Intelligence', www.who.int/ethics/topics/big-data-artificial-intelligence/en; NITI Aayog, 'National Strategy for Artificial Intelligence' (2018), https://niti.gov.in/national-strategy-artificial-intelligence, at 24–45.

[3] D Leslie, 'Understanding Artificial Intelligence Ethics and Safety' (Alan Turing Institute, 2019), https://perma.cc/7V82-JRNR, at 4. See also M Brundage et al., 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation' (Future of Humanity Institute and others, February 2018), https://perma.cc/46NB-8HS2.

[4] See generally J Fjeld et al., 'Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI' (Berkman Klein Center for Internet & Society, 2020).

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

governance.[5] Some governments have translated these ethical frameworks applicable to data-driven services and technologies into binding laws and regulations (or 'data ethics-related measures').

In some cases, data ethics-related measures can have a trade-restrictive impact. For instance, in order to protect personal privacy, governments could restrict the cross-border transfer and processing of personal data that could be burdensome and inefficient, especially for foreign companies. Governments may also demand mandatory access to vital technical information of companies such as the source code and algorithms of their data-driven technologies so as to ensure they are robust, fair and non-discriminatory. Further, as platforms increasingly use automated processes to moderate online content,[6] governments might desire to scrutinise these algorithms to ensure compliance with domestic censorship laws. Such measures may be more burdensome for foreign companies, especially if they prejudice the safety and integrity of their proprietary technologies. Governments may also prescribe specific domestic standards for data-driven services, which may or may not be compatible with global standards.[7] Such measures can interfere with the cross-border supply of digital services and technologies and thus act as trade barriers.[8] However, to date, neither scholars nor policy experts have examined the interface of international trade law and data ethics. For instance, the World Trade Report 2018 of the World Trade Organization (WTO), which focused on AI, mentioned the word 'ethics' only once.[9]

Given these gaps in the existing literature, this chapter addresses whether international trade agreements, such as the WTO's General Agreement on Trade in Services (GATS), provide sufficient policy space to governments to implement data ethics-related measures, despite their possible trade-restrictive effect. More specifically, this chapter explores the role of general exceptions in GATS (art. XIV) in delineating WTO members'[10] policy space to implement data ethics-related measures. Section II discusses the key principles of data ethics common to various policy frameworks, including the protection of human rights; algorithmic accountability; and ethical design. Further, this section highlights examples of government measures intended to implement these data ethics principles, and if and when such measures have a trade-restrictive impact.

[5] L Floridi and M Taddeo, 'What Is Data Ethics?' (2018) 374 *Philosophical Transactions* 1, at 1.

[6] See Ofcom/Cambridge Consultants, 'Use of AI in Content Moderation' (2019), https://perma.cc/4WA4-NKVA.

[7] See Department for Promotion of Industry and Internal Trade (Government of India), 'Draft Electronic Commerce Policy' (2019), https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf, at 30; N Wilson, 'China Standards 2035 and the Plan for World Domination – Don't Believe China's Hype' (CFR, 3 June 2020), https://perma.cc/K5LX-PDXQ; A Gross et al., 'Chinese Tech Groups Shaping UN Facial Recognition Standards' (*The Financial Times*, 2 December 2019), https://perma.cc/T4VD-A8MD.

[8] See subsection B in Section II.

[9] World Trade Organization, 'World Trade Report 2018: The Future of World Trade: How Digital Technologies are Transforming Global Commerce' (2018), https://perma.cc/7NHM-BCU7, at 32.

[10] Henceforth referred to as 'members'.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

Section III examines the interface of international trade law and data ethics in light of the general exceptions in GATS art. XIV. This section argues that GATS art. XIV contains relevant defences for data ethics-related measures. For instance, members may argue that their measures are necessary to achieve compliance with domestic laws, including privacy laws (GATS art. XIV(c)(ii)) or to protect public morals or maintain public order (GATS art. XIV(a)). An evolutionary interpretation of GATS art. XIV can cover several data ethics concerns. However, regulatory diversity across countries and the evolving nature of data ethics frameworks set out a difficult test for assessing the limits of GATS art. XIV, especially examining the core rationale underlying data ethics-related measures, and identifying the least burdensome and trade-restrictive means to realise policy goals enshrined in data ethics frameworks.

Ultimately, applying international trade agreements to data ethics-related measures offers both possibilities and challenges. For instance, WTO panels[11] can meaningfully apply GATS art. XIV to accommodate data ethics principles within the WTO framework, including by referring to relevant private/transnational technical standards on data-driven services and international/multi-stakeholder norms on data ethics and governance. Similarly, using both technological and legal evidence, panels can apply the necessity test in GATS art. XIV to curtail protectionist measures that governments have disguised as being necessary for implementing data ethics principles. However, panels also face the challenge of balancing dynamic domestic and transnational interests related to ethical data governance. In order to better engage with these possibilities and challenges, this chapter recommends that the WTO should open itself to policy developments in data governance as well as remain abreast of technological advances, especially in the designing and verification of digital technologies and services.

## II IMPLEMENTING DATA ETHICS PRINCIPLES AND THEIR TRADE REPERCUSSIONS

Across the world, governments are developing frameworks and high-level principles on data ethics, particularly for AI-driven sectors.[12] Subsection A of this section discusses certain key principles common to these frameworks such as protection of human rights, including individual privacy; algorithmic accountability; and ethical design. It also provides examples of measures that governments impose when

[11] Henceforth referred to as 'panels'.

[12] See Authority of the House of Lords, 'Regulating in a Digital World' (2019), https://perma.cc/YM3H-FG6B; European Parliament, *A Comprehensive European Industrial Policy on Artificial Intelligence and Robotics*, Doc no. P8_TA-PROV(2019)0081 (12 February 2019); European Commission, 'Ethics Guidelines for Trustworthy AI' (2019), https://perma.cc/37YZ-2E59; OECD, *Recommendation of the Council on Artificial Intelligence*, Doc no. OECD/LEGAL/0449 (22 May 2019); NIST, 'US Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools' (2019), https://perma.cc/Z4G7-TUKJ.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

intending to realise these principles. Subsection B then highlights the potential trade-restrictive impact of certain data ethics-related measures.

### A *Key Principles of Data Ethics*

The fundamental component of all data ethics frameworks is the protection of human rights.[13] Several international and regional instruments highlight the importance of a human rights-centric approach in data governance.[14] Similarly, individual governments specifically recognise the importance of protecting human rights in the use of data-driven technologies.[15] The essence of a human rights-centric approach involves increasing individual control over personal data, and ensuring that all data is used, processed and shared in a manner compliant with fundamental human rights.

In this regard, the human rights-centric approach entails protecting individuals against discrimination, promoting digital access and inclusion, and safeguarding individual privacy.[16] From the perspective of data ethics, privacy is essential at all stages of data management, from ensuring informed consent of individuals in the collection of their personal data to increasing human control over all aspects of data processing, including the choice not to be subject to profiling and automated decision-making. The emergence of big data analytics also raises concerns around group privacy (although it remains debatable if this falls within the scope of personal privacy).[17] Unsurprisingly, various domestic laws and regulations now deal with privacy concerns, including data protection laws.[18]

Data-driven technologies can be used to breach human rights other than the right to privacy in various ways. For example, AI algorithms using training data with sensitive variables such as gender and race often generate biased outcomes or

[13] C Cath and L Floridi, 'The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights' (2017) 23(2) *Science and Engineering Ethics* 449, at 455; IEEE, 'Ethically Aligned Design – First Edition' (2019), https://perma.cc/6VZ2-EXNC, at 10. In the specific context of AI, see Fjeld et al., note 4 above.

[14] *Progress Report of the United Nations High Commissioner for Human Rights on Legal Options and Practical Measures to Improve Access to Remedy for Victims of Business-Related Human Rights Abuses*, UN Doc A/HRC/29/39 (May 2015); *Montreal Declaration for Responsible Development of Artificial Intelligence* (2018); OECD, note 12 above.

[15] Personal Data Protection Commission Singapore, 'A Proposed Model for Artificial Intelligence Governance Framework' (January 2019), at 6; Department of Industry, Innovation and Science (Government of Australia), 'AI Ethics Principles' (2019), www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles; European Commission, note 12 above.

[16] United Nations, 'A Human-Rights Based Approach to Data' (2018), https://perma.cc/AX88-85VN.

[17] L Taylor, 'Group Privacy: Big Data and the Collective' (MyData 2017, 24 September 2017), www.youtube.com/watch?v=BsZ05MVFXLU.

[18] For further details, see UNCTAD, 'Summary of Adoption of E-Commerce Legislation Worldwide', https://perma.cc/M7MS-E8AF.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

decisions that adversely affect the fundamental rights of minority groups.[19] Big data analytics can be used to identify and then persecute political minorities or dissidents.[20] Further, governments increasingly use automated algorithms to filter content online, potentially harming the right to freedom of expression and access to information.[21]

A human rights-centric approach in data governance has implications for both governments and the private sector. For instance, governments are required to respect, protect and fulfil human rights[22] by ensuring fair and non-discriminatory use of data-driven technologies for public functions; protecting individuals from potential harms and misuses of data-driven technologies by private sector entities, including enforcement of regulations requiring transparent and non-discriminatory data practices by private entities; and ensuring that private companies provide appropriate remedies to affected individuals. Governments may also require businesses to change specific practices in data management and processing to ensure compliance with a human rights-centric approach in data governance. However, the structural mechanisms by which governments hold the private sector accountable for complying with human rights norms may vary across countries. This difference is attributable to varying perceptions among countries regarding how human rights should be formulated and enforced domestically.

A human rights-centric approach in the governance of data-driven technologies necessitates algorithmic accountability. This means that companies should be held responsible for how their algorithms function, including the decisions taken using them. For instance, in AI-driven technologies, huge datasets (known as training data) are used for predictive analytics and generating decisions in various areas including healthcare, credit reporting, law enforcement, retail and marketing. Several experts argue that increasing algorithmic accountability requires data-driven technologies to be transparent and explainable (i.e. the computer programmers must be able to explain how their algorithms/designs use and process data to generate certain results).[23] This can facilitate rectifying algorithms that generate unfair or discriminatory outcomes.[24] Algorithms can be explained at a systemic level

[19] Fjeld et al., note 4 above, 49; JA Kroll et al., 'Accountable Algorithms' (2017) 165 *University of Pennsylvania Law Review* 633, at 681.

[20] See Human Rights Watch, 'China: Big Data Fuels Crackdown in Minority Region' (HRW, 26 February 2018), https://perma.cc/76QL-RTGK.

[21] L Yuan, 'Learning China's Forbidden History, So They Can Censor It', (*The New York Times*, 2 January 2019), https://perma.cc/3G2D-DUNH.

[22] See generally Committee on Economic, Social and Cultural Rights, *General Comment No 24 on State Obligations under the International Covenant on Economic, Social and Cultural Rights in the Context of Business Activities*, UN Doc E/C.12/GC/24 (10 August 2017).

[23] See AD Selbst and S Barocas, 'The Intuitive Appeal of Explainable Mechanisms' (2018) 87 *Fordham Law Review* 1085, at 1100 – 1120 (on the rationales for explainability of algorithms); Centre for Data Innovation, 'Re: Competition and Consumer Protection in the 21st Century Hearings', Project Number P181201, 15 February 2019.

[24] Ibid.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

(i.e. the logic of an algorithm) or at an individual level (i.e. how the algorithm decides in a specific case),[25] although this distinction remains debatable.[26]

Significant debate exists regarding the extent to which algorithms are or can be explainable and what regulatory mechanisms are needed to achieve the same. Certain experts argue that the transparency of source code/algorithms allows understanding the decision-making rule of the algorithms, but not their functionality in every random set of circumstances.[27] Therefore, they suggest that alternative technological mechanisms must be explored to achieve stronger algorithmic accountability such as verification programs that *ex ante* check if algorithms meet certain specifications (e.g. if they comply with the rule of law), and holding designers/technology companies accountable if and when a program fails to meet those specifications.[28] Others argue that explainability can be achieved through transparency and adequate regulatory inspection of algorithms.[29] On a different note, some experts emphasise that policymakers must be concerned about how data scientists build their datasets and the possible deficiencies in that process rather than solely concentrating on algorithmic accountability.[30]

While it is outside the scope of this chapter to explore these arguments in detail, the diversity of perspectives on algorithmic accountability, including transparency, leads to differing regulatory approaches across countries. This is important because governments are increasingly advocating that transparency and explainability of algorithms is a means to achieving accountability in data-driven technologies.[31] However, certain governments also acknowledge the limitations of transparency and explainability mechanisms in ensuring algorithmic accountability.[32] Separately,

[25] S Wachter et al., 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) *International Data Privacy Law* 76, at 78.

[26] AD Selbst and J Powles, 'Meaningful Information and the Right to Explanation' (2017) 7(4) *International Data Privacy Law* 233, at 239.

[27] M Perel and N Elkin-Koren, 'Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement' (2017) 69 *Florida Law Review* 181, at 184–185, 188; Kroll et al., note 19 above, at 657, 660 (several technologies employ deep learning AI, which constantly self-learns and improvises its design, increasing the difficulty for engineers to explain the outputs of its algorithms).

[28] Kroll et al., note 19 above, at 642. Similarly, see K Martin, 'Ethical Implications and Accountability of Algorithms' (2019) 160 *Journal of Business Ethics* 835, at 844.

[29] DK Citron and F Pasquale, 'The Scored Society: The Due Process for Automation' (2014) 89 *Washington Law Review* 1, 25–30.

[30] D Lehr and P Ohm, 'Playing with the Data: What Legal Scholars Should Learn about Machine Learning' (2017) 51 *UC Davis Law Review* 653, at 663–664.

[31] Personal Data Protection Commission Singapore, note 15 above; Department of Industry, Innovation and Science, note 15 above; European Commission, *Policy and Investment Recommendations for Trustworthy AI* (26 June 2019); European Commission, *Structure for a White Paper on Artificial Intelligence – A European Approach* (2020) (leaked draft), https://perma.cc/M7QH-UEQV, at 16–17; UK House of Lords (Select Committee on Artificial Intelligence), *AI in the UK: Ready, Willing and Able?* (16 April 2018).

[32] UK House of Lords, ibid., 128; Personal Data Protection Commission Singapore, note 15 above, at 6; Department of Industry, Innovation and Science, note 15 above.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

governments may be concerned about the potential trade-offs between transparency and accuracy of algorithms.

The General Data Protection Regulation (GDPR) of the European Union (EU) arguably incorporates important elements of data ethics.[33] GDPR arts 44 and 45 limit data transfers to outside the EU to ensure that all personal data of EU residents is processed according to the highest data protection standards. GDPR art. 12 imposes an obligation on the data controllers to provide concise, transparent, easily understandable and accessible information to individuals regarding how they use personal data, including the extent to which they may use or rely upon personal data for automated decision-making.[34] GDPR art. 22 provides an individual the right not to be subjected to a decision solely based on automated decision-making or profiling,[35] if such a decision has 'legal effects' or 'significantly affects' the concerned individuals. However, significant debate exists regarding whether GDPR art. 22 incorporates a right to explainability of algorithms, for instance, those used in AI technologies.[36]

More recently, other domestic laws have started focusing on data ethics. For instance, the Digital Republic Act in France requires that all algorithmic decision-making by governments should be fully explainable.[37] In the USA, certain senators have proposed an Algorithmic Accountability Act, requiring companies to scrutinise their algorithms for potential risks and biases, thereby enabling greater algorithmic accountability.[38] Finally, certain regional trade agreements include provisions requiring the parties to adopt basic frameworks on data protection.[39] The recently concluded Digital Economy Partnership Agreement between New Zealand, Singapore and Chile includes a specific provision requiring the parties to endeavour to adopt ethical AI governance frameworks, although it only vaguely refers to 'internationally recognised principles or guidelines'.[40]

Another key element in data ethics is ethical design, which is an extension of a human rights-centric approach in data governance. In practice, ethical design requires that all suppliers of data-driven technologies devise and implement technical designs and standards compliant with human rights. For example, privacy-by-

[33] European Commission, 'Ethics and Data Protection' (2018), https://perma.cc/V2C4-8KBK.

[34] See Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation* 2016/679 (6 February 2018), at 10.

[35] Profiling is defined to include any form of automated processing that considers an individual's personal information to analyse their lives. See GDPR art. 4(4).

[36] See Wachter et al., note 25 above; Selbst and Powles, note 26 above; L Edwards and M Veale, 'Slave to the Algorithm? Why a "Right to Explanation" Is Probably Not the Remedy You're Looking For' (2017) 16 *Duke Law & Technology Review* 18.

[37] See L Edwards and M Veale, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' (May/June 2018) *AI Ethics* 46, at 48.

[38] See Algorithmic Accountability Act of 2019 (Proposed Bill), https://perma.cc/V5UQ-LZ53.

[39] See M Wu, 'Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System' (2017) ICTSD, at 25.

[40] Digital Economy Partnership Agreement (DEPA), art. 8.2.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

design and security-by-design measures require digital service suppliers to use digital technologies and implement corporate policies that, by default, ensure data privacy and security. This can be instrumental in protecting personal data and increasing trust in data-driven technologies. Further, as ethical design focuses on technologically robust solutions, it promotes more reliable and sustainable outcomes in comparison to prescriptive data localisation measures or mandatory use of indigenous technical standards. GDPR art. 25 requires all digital service suppliers in the EU to adopt EU data protection principles by design and by default.

In practice, however, implementing ethical design is difficult. This challenge arises as the appropriate standards and benchmarks in the digital sector remain controversial, both in terms of regulatory practices and industry practices. For instance, with respect to privacy, considerable debate exists regarding whether the GDPR should be considered a global standard.[41] Similarly, technical standards developed by leading digital powers such as the USA and China are often market competitors, especially for AI-driven services.[42] Further, while laws and regulations tend to be ambiguous in their meaning (e.g. what is personally identifiable information in a privacy law), engineering models are highly dependent on precision of definitions in designing robust and reliable technologies.[43]

### B *Trade Implications of Data Ethics-Related Measures*

As discussed in Section I, certain data ethics-related measures may be trade-restrictive as they hinder the cross-border supply of digital services, thereby breaching members' obligations in WTO agreements. Some examples include: (i) restrictions on data processing or transfers; (ii) prescribing specific technical standards for digital services and products; and (iii) requiring digital technology providers to submit their algorithms, source code and other vital technical information for government scrutiny/audit.

Governments may impose restrictions on cross-border data flows/processing or even require local storage and processing of data in sensitive sectors, to safeguard individual privacy rights. Some data protection laws even restrict the use of personal data for profiling. In other cases, regulatory approvals may be required to process sensitive data outside of the borders of a country. These measures typically increase costs, especially for foreign companies, lacking local data storage or processing capabilities.[44] When the regulatory requirements for trans-border data transfers/

[41] See generally C Ryngaert and M Taylor, 'The GDPR as Global Data Protection Regulation?' (2020) 114 *AJIL Unbound* 5.

[42] A Roberts et al., 'Toward a Geoeconomic Order in International Trade and Investment' (2019) 22(4) *Journal of International Economic Law* 655, at 673–675.

[43] See K Nissim et al., 'Bridging the Gaps Between Computer Science and Legal Approaches to Privacy' (2018) 31(2) *Harvard Journal of Law & Technology* 689.

[44] N Mishra, 'Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?' (2020) 19 *World Trade Review* 341, at 344–346.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

processing are administered in an unfair or unreasonable manner, they may be inconsistent with domestic regulation provision in GATS art. VI. Further, data processing restrictions may affect the development and accuracy of AI technologies as they prevent data accumulation on a global scale, especially affecting foreign, multi-national suppliers. Such measures may be considered discriminatory against foreign services or service suppliers, potentially breaching national treatment obligation in GATS art. XVII. Under the GDPR, digital service suppliers in the EU face several restrictions in transferring and processing personal data of EU residents abroad (except for a select group of countries that the EU identifies as having an adequate framework of data protection).[45] This restriction on the transfer of personal data to non-EU countries may be inconsistent with the most favoured nation obligation in GATS art. II.

As data-driven services have become common, several governments have started prescribing domestic technical standards, especially in AI-related sectors. These technical standards may be imposed for a variety of reasons, including ensuring that digital technologies are robust and secure, thereby reducing the chances of misuse of data. In the future, governments may prescribe standards that they consider compliant with ethical design requirements. However, if such prescribed standards are incompatible with competitive global standards or extremely onerous to implement, they create barriers for foreign services and service suppliers. In such scenarios, domestic technical standards may violate disciplines on domestic regulation under GATS art. VI.

Requirements imposed on digital technology providers to submit their algorithms and source code for government scrutiny/audit could have an underlying data ethics rationale, but such measures could also be trade-restrictive.[46] For instance, such measures may restrict entry of foreign competitors in domestic markets, thereby breaching national treatment obligation contained in GATS art. XVII. Additionally, such measures can prejudice the security/reputation of global data operations of digital suppliers, thereby violating obligations on domestic regulation in GATS art. VI. For instance, governments can implement such measures unreasonably or unfairly to deliberately harm the commercial interests of foreign players, including sharing their vital technical information with domestic competitors.[47]

[45] GDPR, arts. 44–45. See also 'Adequacy Decisions' (*European Commission*), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[46] See J Vainan, 'Microsoft Just Built a Special Version of Windows for China' (*Fortune*, 23 May 2017), https://perma.cc/WG34-F7FK; B Darrow, 'IBM Gives China Sneak Peek of Software Source Code: Report' (*Fortune*, 16 October 2015), https://perma.cc/F2N5-6MRE.

[47] Such a measure could also violate the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) art. 39, for example, if the measure affects vital commercial interests of foreign companies by increasing the chances of trade secret theft. However, this chapter does not cover justifications of data ethics-related measures under TRIPS. See White House, 'How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World' (June 2018), https://perma.cc/4ZE6-FQ89. See also JY Qin, 'Forced Technology Transfer and the US–China Trade War: Implications for International Economic Law' (2019) 22(4) *Journal of International Economic Law* 743, at 745–746.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

Additionally, in rare scenarios, countries may implement extreme measures banning a certain kind of data-driven technology to prevent abuse of human rights. For example, given the potential dangers and abuses of facial recognition technology, a government could potentially ban commercial software facilitating facial recognition, especially from foreign companies. Such measures may be in conflict with obligations on market access and non-discrimination under GATS.

## III DEFENDING DATA ETHICS-RELATED MEASURES UNDER GATS GENERAL EXCEPTION

Although data ethics-related measures can violate obligations contained in WTO treaties, governments can argue that they protect vital public interests, including protecting privacy and addressing other ethical concerns regarding the processing and sharing of data, under the general exceptions contained in GATS art. XIV. While a significant amount of scholarship has discussed the justification of privacy laws under GATS art. XIV(c)(ii),[48] the role of GATS art. XIV(a) (the public morals/ public order exception) in facilitating other public interests related to data ethics such as protecting against discrimination, facilitating technical robustness and security of technologies, and ensuring appropriate online content moderation remains unexplored. Therefore, after highlighting the relevance of GATS art. XIV(c)(ii) and GATS art. XIV(a) in justifying data ethics-related measures in subsection A of this section, subsection B focuses on how GATS art. XIV(a) applies to data ethics-related measures. Finally, subsection C discusses the various possibilities and challenges involved in accommodating data ethics-related measures within the WTO/GATS framework.

This section argues that GATS art. XIV can play a role in preserving the policy space necessary for members to impose data ethics-related measures. For instance, under GATS art. XIV(c)(ii), members may argue that certain data ethics-related measures are necessary to achieve compliance with domestic laws, especially data protection/privacy laws. Similarly, under the public morals/public order exception in GATS art. XIV(a), panels have generally interpreted ‘public morals’ broadly in line with domestic values/culture; thus, data ethics-related measures can generally qualify under GATS art. XIV(a). However, to ensure a holistic assessment under GATS art. XIV, panels must adopt a cautious, well-reasoned and coherent standard of review in evaluating the necessity of data ethics-related measures under GATS art. XIV. This would entail panels considering both the possibility of accommodating data ethics principles within the GATS framework (e.g. through a meaningful interpretation and application of the exception) and the challenge of balancing

[48] See RH Weber, ‘Regulatory Autonomy and Privacy Standards under the GATS’ (2012) 7 *Asian Journal of WTO and International Health Law & Policy* 25; S Yakovleva and K Irion, ‘The Best of Both Worlds: Free Trade in Services and EU Law on Privacy and Data Protection’ (2016) 2(2) *European Data Protection Law Review* 191.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

(often conflicting) domestic and international perspectives on data governance (e.g. in conducting a holistic weighing and balancing test on the various regulatory means adopted to achieve a data ethics-related policy objective). The ability of the WTO to remain open to relevant policy and technological developments related to data-driven technologies (including relevant multi-stakeholder/transnational norms and standards) will be crucial in ensuring that the GATS framework can support genuine and legitimate data ethics-related measures.

## A *Applying General Exceptions to Justify Data Ethics-Related Measures*

### 1 Relevance of GATS Art. XIV(c)(ii)

GATS art. XIV(c)(ii) is likely to be relevant in justifying data ethics-related measures aimed at protecting individual privacy. Under GATS XIV(c)(ii), a measure violating GATS obligations can be justified if: (a) it is implemented to secure compliance with domestic 'laws and regulations',[49] including those 'relat[ing] to' (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; (b) the above 'laws and regulations' are consistent with WTO law; and (c) the measure is necessary to secure compliance with these laws and regulations.[50]

GATS art. XIV(c)(ii) can be interpreted in an evolutionary manner to cover privacy concerns.[51] For instance, 'protection of privacy of individuals' in GATS art. XIV(c)(ii) could potentially cover measures preventing unauthorised online surveillance of individuals or indiscriminate use of personal data by companies without informed user content. Similarly, data processing outside one's borders may be restricted to prohibit illegal third-party use of personal data. Under GATS art. XIV(c)(ii), members must also demonstrate that the domestic law the measure seeks to achieve compliance with should be consistent with WTO law. While privacy laws are not per se inconsistent with WTO law, certain elements such as discriminatory or ambiguous conditions for cross-border data transfers may violate WTO law.[52] Group privacy concerns arguably do not fall under this exception as deidentified/anonymised data is not generally considered 'personal data', although this data can be used to discriminate against specific groups of individuals. These concerns are more likely to be addressed under GATS art. XIV(a), as discussed next.

[49] See AB Report, *Mexico – Taxes on Soft Drinks* [79] ('laws and regulations' refers to domestic laws and regulation, and not international law, unless it is incorporated into domestic law).

[50] Panel Report, *Colombia – Ports of Entry* [7.514]; AB Report, *US – Shrimp (Thailand)* [7.174]. See also AB Report, *Korea – Various Measures on Beef* [157]; AB Report, *Thailand – Cigarettes (Philippines)* [177]; AB Report, *US – Gambling*, [6.536] – [6.537].

[51] For evolutionary interpretation, see AB Report, *US – Shrimp* [129].

[52] For a more detailed analysis, see Mishra, note 44 above, at 352.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

## 2 Relevance of GATS Art. XIV(a)

When data ethics-related measures do not specifically relate to personal privacy or achieving compliance with other domestic laws, they are more likely to be justified under GATS art. XIV(a) that allows measures: (a) necessary to protect public morals or to maintain public order. The public order exception may be invoked only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society. Further, members may rely on GATS art. XIV(a) in addition to GATS art. XIV(c)(ii) in justifying their data ethics-related measures.

The terms 'public morals' and 'public order' are distinct. However, panels have generally taken the view that 'to the extent that both concepts seek to protect largely similar values, some overlap may exist'.[53] 'Public order' is defined as 'a genuine and sufficiently serious threat' to 'one of the fundamental interests of society'.[54] Public morals is an undefined term; therefore, panels could theoretically interpret public morals with reference to international norms or the domestic values/culture of the country or both. Although this conflict between international/universal values and domestic values remains debatable,[55] WTO tribunals have generally shown an inclination to consider local values in determining the meaning of 'public morals'. In fact, in the *US – Gambling* dispute, the panel held that 'public morals' in GATS art. XIV(a) 'denotes standards of right and wrong conduct maintained by or on behalf of a community or nation', and such standards 'can vary in time and space, depending upon a range of factors, including prevailing social, cultural, ethical and religious values'.[56]

The WTO tribunals have generally applied GATS art. XIV(a) in a broad, flexible and evolutionary manner.[57] For instance, in *China – Publications and Audiovisual Products*, the Appellate Body (AB) held that censorship of printed and digital content fell within the scope of 'public morals' in GATS art. XIV(a).[58] In *US – Gambling*, 'public morals' was interpreted to cover public morals and public order concerns related to online gambling (including money laundering).[59] In *EC – Seals*, the AB held that the term 'public morals' covered animal welfare concerns.[60] In *Brazil – Taxation*, the panel held that a measure imposed to bridge the digital divide and

[53] See Panel Report, *US – Gambling* [6.648].

[54] GATS, art. XIV(a), note 5.

[55] M Wu, 'Free Trade and the Protection of Public Morals: An Analysis of the Newly Emerging Public Morals Clause Doctrine' (2008) 33 *Yale Journal of International Law* 215; S Charnovitz, 'The Moral Exception in Trade Policy' (1998) 38 *Vanderbilt Journal of International Law* 689, at 743.

[56] Panel Report, *US – Gambling* [6.461].

[57] See generally G Marceau, 'Evolutive Interpretation by the WTO Adjudicator' (2018) 21(4) *Journal of International Economic Law* 791. For a discussion of WTO disputes on public morals, see RY Simo, 'Trade and Morality: Balancing Between the Pursuit of Non-Trade Concerns and the Fear of Opening the Floodgates' (2019) 51 *George Washington International Law Review* 407.

[58] Panel Report, *China – Publications and Audiovisual Products* [7.759].

[59] AB Report, *US – Gambling* [296].

[60] AB Reports, *EC – Seal Products* [5.199].

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

promote social inclusion in Brazil fell within the scope of 'public morals'.[61] In *Colombia – Textiles*, the panel held that a domestic tariff intended to combat money laundering in Colombia fell within the scope of 'public morals'.[62]

Governments have significant freedom in deciding how to define and achieve public morality and public order. In *EC – Seals*, the panel identified two steps in assessing measures under the public morals exception: first, if the stated policy concern actually existed in the society and, second, if it fell within the scope of 'public morals'.[63] However, in the same dispute, the AB held that it is not necessary for the tribunal to identify the existence of a specific risk to public morals[64] or identify the exact content of public morals at issue (thus implying that variations of public morals exist depending on the member's values).[65] Further, members have the right to set different levels of protection to address identical moral concerns.[66] Arguably, a similar standard of review may apply when members impose measures necessary for maintaining public order. Although the requirement of a genuine and serious threat is a high threshold, members are likely to have sufficient discretion in determining the fundamental interest of their society. For instance, a member desiring to control the domestic internet activities of their residents could argue that restricting data transfers/processing is required for maintaining 'public order'.

Given the flexible interpretation of GATS art. XIV(a), data ethics-related measures are likely to fall within the scope of this provision. First, governments could argue that algorithmic accountability and ethical design are important elements of domestic public policy such as protecting social order and protecting consumers from harm. Second, the adoption of a human rights-centric approach can be a defining element of a society's public morals and constitute a fundamental public interest. For example, in order to protect minority groups from algorithmic discrimination, a government must be able to scrutinise the algorithms/source code, thereby qualifying under 'public morals' and 'public order'. Third, privacy is considered to be a 'moral' issue in many societies because of its connection with socio-cultural and religious values.[67] For example, sexual preferences and religious affiliation are considered highly intimate information in many societies. Finally, certain governments may argue that their data ethics-related measures are connected to human rights recognised in international instruments and declarations of the international policy community on data governance.[68] While panels are unlikely to accept public

[61] Panel Report, *Brazil – Taxation* [7.591]–[7.592].

[62] Panel Report, *Colombia – Textiles* [7.338]–[7.339]; AB Report, *Colombia – Textiles* [5.105].

[63] Panel Report, *EC – Seal Products* [7.381]–[7.383].

[64] AB Report, *EC – Seal Products* [5.198].

[65] AB Report, *EC – Seal Products* [5.199].

[66] AB Report, *EC – Seal Products* [5.200].

[67] See JQ Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 *Yale Law Journal* 1151.

[68] Scholars have generally advocated that 'public morals' could include universal human rights. See C Glinski, 'CSR and the Law of the WTO: The Impact of *Tuna Dolphin II* and *EC–Seal Product*' (2017) 1 *Nordic Journal of Commercial Law* 121, at 133.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

morals or public order exception as a basis for enforcing international human rights,[69] they are likely to attempt to interpret GATS art. XIV(a) in a manner that respects human rights and international public policy.

### B *Applying the Public Morals/Public Order Exception to Data Ethics-Related Measures*

If a data ethics-related measure qualifies under GATS art. XIV(a) or GATS art. XIV(c)(ii), the panel must examine its necessity to achieve the underlying policy objective under a 'weighing and balancing test'. This subsection focuses on the necessity of data ethics-related measures to protect public morals or maintain public order in accordance with the 'weighing and balancing test'.

The first step in this test is assessing the contribution of the measure to the policy objective under GATS art. XIV – that is, the nexus between the measure and the policy objective under GATS art. XIV[70] – for instance, by looking at the design, content, structure and expected operation of the data ethics-related measure.[71] For example, if a member requires companies to provide their source code or algorithms to verify them for bias (e.g. discriminating against minorities) or other privacy loopholes (particularly, group privacy concerns), the panel will examine if this requirement contributes to protecting public morals or maintaining public order under GATS art. XIV(a). From a technological perspective, this assessment can be difficult as the efficacy of transparency/disclosure of algorithms and source code to understand the underlying logic and discriminatory outcomes in algorithmic decision-making remains debatable.[72] For complex AI, such disclosure requirements can also be counterproductive; for example, in autonomous vehicles, requiring access to the algorithms could compromise the security of the digital technologies. As explainability of algorithms improves with technological developments (especially the development of explainable AI or XAI), panels can make better assessments by seeking additional expert technical evidence on relevant issues.

Similarly, questions may arise regarding whether restrictions on cross-border data flows contribute to achieving the key principles of data ethics. Several studies indicate that severe restrictions on data flows are generally ineffective in enhancing the privacy or security of data-driven technologies.[73] Similarly, locating data within

[69] G Marceau, 'WTO Dispute Settlement and Human Rights' (2002) 13(4) *European Journal of International Law* 753, at 761, 777, 813–814; SM Zonaid, 'Trading in Human Rights: Questioning the Advance of Human Rights into the World Trade Organization' (2015) 27 *Florida Journal of International Law* 261, at 286.

[70] AB Report, *US – Gambling* [292].

[71] AB Report, *EC – Seal Products* [5.302].

[72] See discussion in subsection A, Section II.

[73] See T Maurer et al., 'Technological Sovereignty: Missing the Point?', in M Maybaum et al. (eds), *Architectures in Cyberspace* (Tallinn, NATO CCD COE Publications, 2015), at 53, 61–62; K Komaitis, 'The "Wicked Problem" of Data Localization' (2017) 3(2) *Journal of Cyber Policy* 355, at 361–362.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

one's borders does not automatically increase control or access to data. To the contrary, such measures increase the possibility of unauthorised surveillance and violation of human rights as well as interfering with the development of a healthy and competitive domestic digital market, especially when few companies (potentially state-controlled) own all the domestic data centres. However, easy access to local data servers may facilitate easier regulatory enforcement (e.g. pursuing action against companies that fail to comply with data ethics-related measures).

To facilitate a higher standard of data ethics, members may impose domestic regulations requiring technology companies to comply with internationally recognised technical standards, or adopt designs that protect privacy and security by default and/or use certification mechanisms to verify compliance with these ethical design requirements.[74] In comparison to blatant cross-border data transfer restrictions, these requirements appear more effective in facilitating digital inclusion, preventing disinformation campaigns and ensuring technologically robust solutions. Therefore, such measures are more likely to contribute to protecting public morals and maintaining public order.

The next step under the weighing and balancing test is assessing the trade-restrictiveness of the data ethics-related measure; that is, the restrictive impact of the measure on international commerce.[75] This step involves an assessment not only of the sector affected directly by the measure but also other sectors. For example, as data-driven services are used across several industries, restrictions on cloud computing services (e.g. mandatory compliance with domestic technical standards or data/security certifications) can potentially impact several sectors.[76]

Finally, in applying the weighing and balancing test, panels will take into account any alternative less trade-restrictive measures proposed by the complainant. The key factors examined are whether such alternatives are reasonably available to and feasible to implement.[77] Further, any proposed alternatives must achieve an equivalent level of protection of the stated policy objective as the imposed measure.[78] With regard to regulating certain aspects of the digital sector, self-regulatory (or market-driven) approaches may be more effective and efficient than highly prescriptive laws and regulations.[79] For example, rather than imposing specific technical standards, competitive standards developed by the industry in sectors such as AI are more likely

[74] IEEE, note 13 above, at 28.

[75] AB Report, *China – Publications and Audiovisual Products* [306].

[76] See JP Meltzer, 'The Impact of Artificial Intelligence on International Trade' (2018), https://perma.cc/A3H7-FXVB (in the context of AI-driven technologies); A Goldfarb and D Trefler, 'AI and International Trade' (2017), https://perma.cc/5Z9K-29EK, at 24–29.

[77] AB Report, *US – Gambling*, [308]; AB Report, *China – Publications and Audiovisual Products* [326]–[327]; AB Report, *EC – Seal Products* [5.279].

[78] See AB Report, *Brazil – Retreaded Tyres* [156]; AB Report, *China – Publications and Audiovisual Products* [246].

[79] See S-Y Peng, 'The Rule of Law in Times of Technological Uncertainty: Is International Economic Law Ready for Emerging Supervisory Trends?' (2019) 22 *Journal of International Economic Law* 1, at 13–15.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

to be transparent and secure. Similarly, instead of restricting data-driven technologies through unreasonable regulations on data processing, countries could recognise market-driven verification mechanisms that certify compliance with robust standards on ethical design.

Despite the growing popularity of these market-driven mechanisms, panels are likely to consider them as, at best, complementary measures rather than alternatives to prescriptive laws and regulations.[80] This is because countries may be concerned about the robustness of the representativeness of private/multi-stakeholder standards, especially when developed without sufficient government oversight.[81] This would be the case even if the private/multi-stakeholder standards are robust and generally considered industry best practices. Further, verification/certification mechanisms could be very difficult and expensive for developing countries to adopt and monitor and thus not feasible. Therefore, at least in the current scenario, most market-driven or self-regulatory alternatives to data ethics-related measures are likely to fail to satisfy the threshold in GATS art. XIV. The same argument could also be made for technological mechanisms to ensure greater algorithmic accountability (as discussed in subsection A, Section II). In such cases, panels are likely to find more prescriptive measures such as mandatory disclosure of source code/algorithms compliant with GATS art. XIV.

If a trade-restrictive measure provisionally satisfies the necessity test under GATS art. XIV(a), it must further be consistent with the chapeau:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on international trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures.

The chapeau prevents members from abusing exceptions contained in the subsections of GATS art. XIV and ensures that members implement all measures in good faith.[82] It requires an enquiry into the 'design, architecture, and revealing structure of a measure'[83] to assess if the measure violates the GATS art. XIV chapeau in 'its actual or expected application'.[84] For example, if a measure deliberately prohibits foreign service suppliers from obtaining licences or authorisations to provide their services on grounds that their algorithms or technical standards do not meet the adequate threshold (irrespective of the quality and robustness of the standard/algorithms), then it might be inconsistent with the GATS art. XIV

[80] See AB Report, *Brazil – Retreaded Tyres* [151], [211]; Panel Report, *China – Rare Earths* [7.186]; Panel Report, *Australia – Plain Packaging* [7.1384]–[7.1391].

[81] L DeNardis and M Raymond, 'The Internet of Things as a Global Policy Frontier' (2017) 15 *UC Davis Law Review* 475, at 493.

[82] AB Report, *US – Shrimp* [158].

[83] AB Report, *EC – Seal Products* [5.302].

[84] Ibid.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

chapeau. Another example of a potential violation is, when governments illegally share vital technical information regarding foreign digital technologies with domestic competitors, making it harder for foreign companies to compete in that market and further causing potential intellectual property losses.

### C *Data Ethics and International Trade Law: Possibilities and Challenges*

The previous subsections indicate that although GATS art. XIV can justify data ethics-related measures, several questions remain unanswered regarding the extent to which GATS art. XIV provides sufficient policy space for members to impose data ethics-related measures. For instance, should panels place any limits in defining 'public morals' or 'public order' under GATS art. XIV(a) in accommodating data ethics concerns? Given the technological and policy uncertainty, what standard of review should panels adopt under GATS art. XIV in reviewing data ethics-related measures? Should panels be completely deferential to the risk assessment made by governments in relation to their data ethics-related measures or should they conduct a more substantive assessment? What tools should the panels use in this assessment? How will the growth of new technological mechanisms such as XAI or market-driven standards and verification mechanisms impact the assessment of data ethics-related measures under GATS art. XIV?

Data ethics-related measures are typically nuanced in nature. To understand these measures holistically, governments must focus on both their legal/policy implications and technological impact. Thus, in assessing data ethics-related measures under GATS, panels must follow a well-reasoned, cautious and coherent standard of review that looks at both the technological and legal evidence. However, given the limited technical expertise of panels, they should refrain from engaging in a de novo review of data ethics-related measures and cautiously use technical expert opinions.

In applying this standard of review, two routes are possible. First, in assessing whether certain data ethics-related measures relate to GATS art. XIV, panels can, in addition to considering local values and policy preferences of members, pay regard to developments in the international/multi-stakeholder policy community on data governance. This route is not entirely unrealistic given that data ethics issues implicate several transnational policy concerns and not just domestic concerns. Further, such an approach is also helpful given the critical role of multi-stakeholder institutions in promoting data ethics, as discussed in subsection A, Section II. In *Brazil – Taxation*, for instance, the panel considered not only the importance of the digital divide as a domestic policy objective within Brazil, but also discussed its relationship with the Millennium Development Goals.[85] However, this route is

[85] G Moon, 'A "Fundamental Moral Imperative": Social Inclusion, the Sustainable Development Goals and International Trade Law After Brazil- Taxation' (2018) 52(6) *Journal of World Trade* 995, at 1004.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

politically and legally challenging in circumstances where local values conflict with international/multi-stakeholder norms. WTO tribunals do not have the capacity or mandate to determine the appropriate data ethics frameworks for individual members. Therefore, if a country considers that certain international/multi-stakeholder norms are not aligned with its policy preferences, trade tribunals must not interfere, even when those international/multi-stakeholder norms can lead to better outcomes for data ethics. This limitation, however, may lead to scepticism towards the WTO; that is, the panels cannot make decisions that clearly support a human rights-centric approach in data governance.

The second route is adopting a more stringent weighing and balancing test in assessing data ethics-related measures under GATS art. XIV(a).[86] The necessity test can be effective in detecting discriminatory or unnecessarily trade-restrictive measures.[87] For example, looking at the technical aspect of the measure (i.e. inviting expert evidence on whether a data ethics-related measure is actually capable of achieving important policy goals) is less controversial than examining the moral elements of the measure, which often implicates sensitive political or cultural questions. This approach, however, does not necessarily allow panels to consider innovations in the digital sector such as the potential role of technological mechanisms in the verification of data-driven technologies. For instance, engineers and computer scientists designing data-driven services can build *ex ante* verification mechanisms that ensure that the program/algorithm meets the specifications in domestic laws and processes.[88] Panels are unlikely to consider such mechanisms as a viable less trade-restrictive alternative under GATS art. XIV, especially when the defendant governments do not consider them as effective as regulatory access to source code/algorithms. Similarly, panels are unlikely to consider strict scrutiny/audits of training data by the private companies themselves a fool-proof mechanism to ensure fair and transparent outcomes in algorithmic decision-making, especially when governments restrict automated decision-making in risky and sensitive sectors.[89] However, as such market-based, technological mechanisms become more fit-for-purpose and reliable, they could be considered as more viable and qualify as potential candidates as less trade-restrictive alternatives under GATS art. XIV. Such mechanisms are also likely to be considered credible if they are developed and implemented by the private sector in collaboration with regulatory bodies, especially for countries with sufficient resources to hold private companies accountable for their poor data ethics practices.[90]

[86] S Nuzzo, 'Tackling Diversity Inside WTO: GATT Moral Clause After Colombia – Textiles' (2017) 10 (1) *European Journal of Legal Studies* 267, at 290–292; JC Marwell, 'Trade and Morality: The WTO Public Morals Exception After Gambling' (2006) 81 *New York University Law Review* 802, 805.

[87] See generally Mishra, note 44 above.

[88] Kroll et al., note 19 above, at 642.

[89] Wachter et al., note 25 above, at 99.

[90] See C Sabel et al., 'Regulation under Uncertainty: The Coevolution of Industry and Regulation' (2018) 12 *Regulation and Governance* 371, at 373, 375 (arguing that uncertainties can prompt coordination among firms and between firms and regulatory bodies).

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press

In the long run, the WTO needs to respond to the predominantly decentralised nature of data governance. For example, the WTO needs to adopt new rules and institutional mechanisms that allow collaboration between governments, technology companies and relevant multi-stakeholder or transnational organisations dealing with data governance. An important example in this regard is the development of technical standards on AI software by the private sector. Currently, GATS does not provide sufficient room for such standards for services.[91] However, at domestic/regional levels, several governments are coordinating with the private sector on certain aspects of data governance such as development of AI standards. These multi-stakeholder mechanisms could eventually grow transnationally (especially among like-minded countries) and can be facilitated through WTO committees. Eventually, such a broad-based approach could ensure that the WTO plays a more meaningful role in promoting good global data ethics practices and robust digital technologies.

## IV CONCLUSION

This chapter investigated whether the general exceptions in GATS provide adequate policy space to governments to impose data ethics-related measures. In evaluating data ethics-related measures under GATS art. XIV, panels can take into account both international norms and best practices as well as local values or socio-cultural preferences, especially if they are aligned with each other. This chapter also demonstrates that panels can adopt a well-reasoned, cautious and coherent standard of review in assessing the necessity of data ethics-related measures under GATS art. XIV by holistically looking at both legal and technological evidence in each step of the weighing and balancing test. However, the possibility of panels considering a wider range of private sector-driven or multi-stakeholder mechanisms as alternatives to prescriptive data ethics-related measures, especially new verification technologies and technical standards, currently remains limited. Therefore, moving forward, the WTO framework must better co-opt international/multi-stakeholder norms and standards applicable to data-driven services so as to remain more open and responsive to the dynamic policy developments in data governance.

[91] GATS art. VI:4 read with art. VI:5 allows panels to only take into account technical standards of multilateral institutions. A possible route is exploring technical barrier to trade-like provisions for trade in services.

https://doi.org/10.1017/9781108954006.014 Published online by Cambridge University Press