10

The Algorithmic Learning Deficit

Artificial Intelligence, Data Protection and Trade

*Svetlana Yakovleva and Joris van Hoboken**

A INTRODUCTION

Commercial use of personal and other data facilitates digital trade and generates economic growth at unprecedented levels. A dramatic shift in the composition of the top twenty companies by market capitalisation speaks vividly to this point. While, in 2009, 35 per cent of those companies were from the oil and gas sector, in 2018 – just nine years later – 56 per cent of those companies were from the technology and consumer services sectors.[1] Meanwhile, the share of oil and gas companies, a pillar among traditional industries, declined to just 7 per cent. The share of digitally deliverable services in global services exports more than doubled in the last thirteen years: it increased from USD 1.2 trillion in 2005 to USD 2.9 trillion in 2018.[2]

Data also constitutes a crucial resource for the development, continuous refinement and application of artificial intelligence (AI). The availability of data and its free flow across borders are often viewed as pre-requisites for the development and flourishing of AI technology.[3] However, in the context of AI, it is not the data itself, but the knowledge and insights obtained with the help of AI algorithms from that data (in other words, the 'fruits' of the data) that constitute the main added value.

* Svetlana Yakovleva is a Postdoctoral Researcher at the Institute for Information Law (IViR), University of Amsterdam and Senior Legal Adviser at De Brauw Blackstone Westbroek, Amsterdam. Contact: mail@svyakovleva.com. Joris van Hoboken is Associate Professor at the Institute for Information Law (IViR), University of Amsterdam and Professor of Law at the Interdisciplinary Research Group on Law Science Technology & Society (LSTS), Vrije Universiteit Brussel. Contact: j.v.j.vanhoboken@uva.nl.

[1] UNCTAD, *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries* (New York/Geneva: United Nations Publications, 2019), at 17.

[2] Ibid., at 48.

[3] See, e.g., S. A. Aaronson, 'Data Minefield? How AI Is Prodding Governments to Rethink Trade in Data', in CIGI (ed), *Special Report: Data Governance in the Digital Age* (Waterloo: CIGI, 2018).

Learning, or 'digital intelligence', in the words of UNCTAD, is crucial for the market of big data. One of the upshots of this is that without the necessary infrastructure and technologies, data concerning individual persons or even aggregated data cannot by itself generate value. It is the 'learning', and not raw data itself, that constitutes a valuable economic resource and can be used in targeted online advertising, the operation of electronic commerce platforms, the digitisation of traditional goods into rentable services and the renting out of cloud services.[4] For example, personalisation, which is an important component in the production, marketing and distribution of online services, uses AI systems to transform individuals' online behaviour, preferences, likes, moods and opinions (all of which constitute personal data, at least in the European Union) into commercially valuable insights.[5] Focusing solely on data in the context of regulatory conversations on AI – both in domestic and international trade contexts – may be misguided.

AI development is at the top of the domestic and international policy agendas in many countries around the world. Just in the last couple of years, more than thirty countries and several international and regional stakeholders, including the European Union (EU), G20 and Nordic-Baltic Region adopted AI policy documents[6] revealing their ambitions to compete for dominance in AI. Digital trade provisions, including rules governing cross-border data flows, access to proprietary algorithms and technology transfers and access to open government data, have taken centre stage in bilateral, regional and international trade negotiations.[7]

Different levels of advancement in digital technologies in general, and in AI specifically, as well as the concentration of data in the hands of a few countries, make international negotiations on digital trade challenging. To illustrate the point, according to the 2019 UNCTAD Digital Economy Report, China and the United States account for 90 per cent of the market capitalisation value of the worlds' seventy largest digital platform companies and 'are set to reap the largest economic gains from AI'.[8] In contrast, the EU accounts for only 3.6 per cent of this market capitalisation.[9] The report further demonstrates that China, the United States and Japan together account for 78 per cent of all AI patent filings in the world.[10] Data – one of the key components of data analytics – is highly concentrated in Asia Pacific

[4] UNCTAD, note 1, at 24 et seqq.

[5] J. Crémer, Y.-A. de Montijoye, and H. Schweitzer, *Competition Policy for the Digital Era* (Luxembourg: Publications Office of the European Union, 2019), at 73.

[6] For an overview, see OECD, AI Initiatives Worldwide, available at www.oecd.org/going-digital/ai/initiatives-worldwide/.

[7] S. Azmeh and C. Foster, 'The TPP and the Digital Trade Agenda: Digital Industrial Policy And Silicon Valley's Influence on New Trade Agreements', LSE Working Paper No 16-175 (2016); J.-A. Monteiro and R. Teh, 'Provisions on Electronic Commerce in Regional Trade Agreements', WTO Working Paper No ERSD-2017-11 (2017). See also Chapter 1 in this volume.

[8] UNCTAD, note 1, at 8–9.

[9] Ibid.

[10] Ibid., at 8–9, 21.

and the United States: 70 per cent of all traffic between 2017 and 2022 is expected to be attributed to these two regions.[11] Representing 87 per cent of the B2B e-commerce, the United States is the market leader in global e-commerce, while China is the leader in B2C e-commerce followed by the United States.[12] As a result, economic value derived from data is captured by countries where companies having control over storage and processing of data reside.[13]

The high concentration of control over AI technologies, digital platforms and data in specific parts of the world raise concerns about 'digital sovereignty' related to control, access and rights of the data and appropriation of the value generated by the monetisation of the data.[14] This issue is not limited to the dynamics of negotiations between developed and developing countries. For example, the new European Commission's Digital Strategy is strongly anchored in the principles of digital sovereignty and shaping technology in a way respecting European values.[15] Public policy interests implicated by international data governance and data flows, indispensable for the global governance of AI, stretch far beyond issues of economic growth and development. They also involve a broader set of national and regional priorities, such as national security, fundamental rights protection (such as the rights to privacy and to protection of personal data) and cultural values, to name just a few. Differences in the relative weight accorded to each such priority when contrasted with the economic and political gains from cross-border data flows have resulted in a diversity of domestic rules governing cross-border flows of information, especially when it relates to personal data, and a diversity of approaches to govern the use of AI in both private and public law contexts.

Against this backdrop, this chapter's aim is twofold. First, it provides an overview of the state of the art in international trade agreements and negotiations on issues related to AI, in particular, the governance of cross-border data flows. In doing so it juxtaposes the EU and the US approaches and demonstrates that the key public policy interests behind the dynamics of digital trade negotiations on the EU's side are privacy and data protection. Second, building on the divergent EU and US approaches to governing cross-border data flows, and the EU policy priorities in this respect in international trade negotiations, this chapter argues that the set of EU public policy objectives weighted against the benefits of digital trade in international trade negotiations, especially with a view to AI, should be broader than just privacy and data protection. It also argues that an individual rights approach has limitations in governing data flows in the context of AI and should be expanded to factor in a

[11] Ibid., at 11.
[12] Ibid., at 15.
[13] Ibid., at 89.
[14] Ibid.
[15] European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, COM(2020) 65 final, 19 February 2020 [hereinafter: White Paper on Artificial Intelligence].

clearer understanding of who wins and who loses from unrestricted cross-border data flows in an age of data-driven services and services production.

The chapter proceeds as follows. The next section maps out the recent developments on digital trade on the international trade law landscape. The third section discusses, from an EU perspective, the limits of data protection in regulating AI domestically and as a catch-all public policy interest counterbalancing international trade commitments on cross-border data flows. The fourth section contains a brief conclusion.

B CROSS-BORDER DIGITAL TRADE AND ARTIFICIAL INTELLIGENCE

The immense potential of data to generate economic value has given rise to a so-called 'digital trade discourse', which, on the one hand, views the freedom of cross-border data flows as one of the pre-requisites of international digital trade and AI-driven innovation and, on the other hand, predicts that restrictions on data flows will hamper economic growth and undermine innovation.[16] This discourse is advanced not only by the United States, which has a strong competitive advantage in digital technologies, and the big tech companies, which invest millions of dollars in lobbying activities on digital trade, but also by the EU.[17]

Policy debates in international trade negotiations on digital trade, relevant in the AI context, revolve around the liberalisation of cross-border data flows in order to enable accumulation of large data sets to train AI systems and restrictions on those data flows in the public interest. The following subsections provide an overview of recent developments in this area.

Countries have not yet achieved a multilateral consensus on the design and scope of digital trade provisions, which have so far only appeared in bilateral and regional trade agreements and have somewhat overshadowed the multilateral efforts of the WTO in this area.[18] Although proposals on electronic commerce in the WTO increasingly focus on barriers to digital trade and 'digital protectionism',[19] the WTO has not yet made any tangible progress on this issue.[20] The discussions continue, however. In early 2019, seventy-six WTO members, including Canada, China, the EU, and the United States, started a new round of negotiations on electronic commerce at the WTO in order to create rules governing e-commerce

[16] UNCTAD, note 1, at 91. For overview and discussion, see S. Yakovleva, 'Privacy Protection (ism): The Latest Wave of Trade Constraints on Regulatory Autonomy', *University of Miami Law Review* 74 (2020), 416–519, at 469 et seqq. See also Chapter 3 in this volume.

[17] Yakovleva, note 16, at 473, 482; UNCTAD, note 1, at 88–89.

[18] M. Burri, 'The Regulation of Data Flows through Trade Agreements', *Georgetown Journal of International Law* 48 (2017), 407–448, at 417.

[19] A. D. Mitchell and N. Mishra, 'Data at the Docks: Modernizing International Trade Law for the Digital Economy', *Vanderbilt Journal of Entertainment and Technology Law* 20 (2018), 1073–1134, at 1111.

[20] See Chapter 1 in this volume.

and cross-border data flows.[21] It remains to be seen how these negotiations will play out. Despite a seemingly firm consensus on the use of the terms 'digital trade' and 'digital protectionism' – the axes around which the discourses governing international negotiations revolve – the value structures underlying these discourses diverge,[22] as the US and the EU examples below will illustrate. The next section on international trade law governance of cross-border data flows then explicates how trade provisions on cross-border data flows, advanced by the US and the EU, mirror this divergence.

In the spirit of its 'digital agenda', the United States has been a pioneer in including provisions on free cross-border data flows in international trade agreements.[23] The United States has managed successfully to advance broad and binding horizontal obligations enabling unrestricted data flows in the digital trade (or electronic commerce) chapters of its recent trade agreements. The Comprehensive and Progressive Agreement on Trans-Pacific Partnership (CPTPP), (where the US led digital trade discussions before its withdrawal from the TPP agreement[24]), the United States–Mexico–Canada Agreement (USMCA) and the Digital Trade Agreement with Japan examples are of trade agreements to contain a binding provision requiring each party to allow (or not to restrict) the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.[25] The US proposal for the ongoing e-commerce talks at the WTO replicates this 'gold standard' provisions on digital trade.[26] All of the earlier mentioned free trade agreements (FTAs) also contain an exception which allows the parties to adopt or maintain measures inconsistent with this obligation to achieve a legitimate public policy objective, provided that the measure (i) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (ii) does not impose restrictions on transfers of

[21] European Commission, '76 WTO Partners Launch Talks on E-Commerce', *News Archive*, 26 January 2019, available at http://trade.ec.europa.eu/doclib/press/index.cfm?id=1974.

[22] Yakovleva, note 16, at 469 et seqq. See also Chapter 12 in this volume, in particular with regard to the position of China.

[23] M. Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation', *UC Davis Law Review* 51 (2017), 65–132, at 99, S. A. Aaronson, 'Redefining Protectionism: The New Challenge in the Digital Age', IIEP Working Paper No 30 (2016), at 59; M. Geist, 'Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards', in CIGI (ed), *Special Report: Data Governance in the Digital Age* (Waterloo: CIGI, 2018).

[24] This provision was included in CPTPP before the US withdrawal from the agreement. The version of the agreement with the United States as a party was known as the Transpacific Partnership Agreement (TPP). See Executive Office of the President, Office of the United States Trade Representative, Letter to the TPP Depository, 30 January 2017.

[25] Article 14.11(2) CPTPP and Article 19.11(1) USMCA. For other agreement containing a similar rule, see Chapter 1 in this volume.

[26] I. Manak, 'US WTO E-Commerce Proposal Reads Like USMCA', *International Economic Law and Policy Blog*, 8 May 2019, available at https://worldtradelaw.typepad.com/ielpblog/2019/05/us-wto-e-commerce-proposal-reads-like-usmca.html.

information *greater than are required* (*necessary* – in the USMCA and US–Japan Digital Trade Agreement) to achieve the objective.[27]

The exception closely resembles the general exception under Article XIV(c)(ii) of the General Agreement on Trade in Services (GATS),[28] a threshold which has been particularly hard to meet in the past.[29] Similar to the general exception clause, the FTA text requires that a measure prima facie inconsistent with the data flow obligation should be subject to a two-level assessment. First, it should pass the so-called 'necessity test', where the necessity of the contested measure is assessed, based on an objective standard of 'necessity' by trade adjudicators. Second, its application should not amount to arbitrary or unjustifiable discrimination or a disguised restriction on trade (pursuant to the chapeau of the general exception provision). Under WTO case law, the 'necessity test' requires that a WTO law–inconsistent measure be the least trade restrictive of all reasonably available alternatives allowing to achieve the same level of protection of a public interest, raised by the claimant in a dispute.[30] In short, just like the GATS general exception, the FTA exception sets a high threshold for justifying a domestic measure inconsistent with relevant trade disciplines. An important difference of the earlier quoted FTA exception from the GATS general exception, however, is that it does not specify the public policy objectives that may be invoked to justify a restriction on the free cross-border data flows. In this sense, the exception is more 'future-proof', as it can rest on any public policy interest that may be implicated by the cross-border data flow obligation in the future, such as cybersecurity or even technological sovereignty (not mentioned in Article XIV GATS exception), provided of course that the measure passes the two-level assessment of the exception.

In addition, the digital trade (electronic commerce) chapters of the earlier mentioned agreements contain an article on the protection of personal information (the term used to refer to personal data in the United States), which contains a mixture of binding and aspirational provisions on the protection of privacy by the parties to the agreements.[31]

[27] Article 14.11(3) CPTPP, Article 19.11(2) USMCA and Article 11 US–Japan DTA contain an almost identical provision. Emphasis added.

[28] General Agreement on Trade in Services, 1869 U.N.T.S. 183; 33 I.L.M. 1167 (1994), entered into force 1 January 1995 [hereinafter: GATS].

[29] P. Delimatsis, 'Protecting Public Morals in a Digital Age: Revisiting the WTO Rulings on *US – Gambling and China – Publications and Audiovisual Products*', *Journal of International Economic Law* 14 (2011), 1–37; I. Venzke, 'Making General Exceptions: The Spell of Precedents in Developing Article XX GATT into Standards for Domestic Regulatory Policy', *German Law Journal* 12 (2011), 1111–1140, at 1118–1119.

[30] For more references, discussion and critique in the privacy and data protection context, see S. Yakovleva, 'Should Fundamental Rights to Privacy and Data Protection Be a Part of EU's International Trade "Deals"?' *World Trade Review* 17 (2018), 477–508; S. Yakovleva, 'Personal Data Transfers in International Trade and EU Law: A Tale of Two "Necessities"', *Journal of World Investment and Trade* 21 (2020), 881–919.

[31] Article 14.8 of CPTPP and Article 19.8 of USMCA. These articles are discussed in more detail in S. Yakovleva, 'Privacy and Data Protection in the EU- and US-led Post-WTO Free Trade

The EU largely shares the 'digital trade' discourse on the benefits of cross-border data flows for global economic growth with the United States and, in principle, supports the idea of regulating cross-border data flows in international trade agreements.[32] Largely but not completely, because there is one important point on which the EU approach diverges very significantly from that of the United States: namely, with regard to the protection of the rights to privacy and personal data. It is for this reason that the EU has until recently been cautious in including provisions on cross-border data flows in its trade agreements.[33] Understanding the EU's domestic framework on the protection of personal data and, in particular, its approach to transfers of personal data outside the European Economic Area (EEA), is essential for explaining its trade policy in the domain of cross-border data flows. Therefore, before delving into the EU's proposed provisions on the latter topic, let us first briefly discuss the EU's domestic regime for transfers of personal data outside the EEA.

The rights to privacy and the protection of personal data are protected as binding *fundamental rights* in the EU.[34] From an EU data protection law perspective, personal data is distinct from other types of information because of its inextricable link to the data source: individuals. One of the pillars of this protection, as the CJEU has ruled,[35] is the restriction on transfers of personal data outside the EEA in order to ensure that the level of protection guaranteed in the EU by the General Data Protection Regulation (GDPR)[36] is not undermined or circumvented as personal data crosses EEA borders.[37] As a consequence of the broad definition of 'personal data', EU restrictions on transfers of personal data apply to a broad range of data that can be essential for developing, fine tuning and application of AI systems. Furthermore, the restrictions also apply to mixed data sets, in which personal and non-personal data are 'inextricably linked' – which, as mentioned earlier, fall under

Agreements', in R. Hoffmann and M. Krajewski (eds), *European Yearbook of International Economic Law* (Berlin: Springer, 2020), 95–115.

[32] For elaborate discussion on the US and EU digital trade discourses, see Yakovleva, note 16, at 469 et seqq.

[33] For more details on the reasons for this, see Yakovleva, note 16, at 492–493. For the first time the EU included binding provisions on cross-border data flows in Article DIGIT 6 of the 2021 EU-UK Trade and Cooperation Agreement.

[34] Respectively Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), OJ L [2000] 364/1.

[35] C-362/14, *Maximilian Schrems* v. *Data Protection Commissioner and Digital Rights Ireland Ltd.* [2015], ECLI:EU:C:2015:650 [hereinafter: *Schrems*], at para. 72. This goal is now explicitly incorporated in Article 44 GDPR.

[36] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), OJ L [2016] 119/1.

[37] Article 44 GDPR; *Schrems*, note 35, para. 72. See also G. González Fuster, 'Un-Mapping Personal Data Transfers', *European Data Protection Law Review* 2 (2016), 160–168, at 168. Restrictions are provided for in chapter V, GDPR. For an overview of restrictions, see Yakovleva, note 31.

the scope of the GDPR.[38] The restrictions do not apply to non-personal data, including non-personal data in mixed data sets, under the condition that those can be separated from personal data. At the same time, the distinction between personal and non-personal data is not set in stone. If, due to technological developments, this anonymised data can be reidentified, it will become 'personal' and the GDPR restrictions will again apply.[39] Some scholars argue that these restrictions limit the cross-border aggregation of data and thus stifle the development of AI.[40]

The GDPR's restrictions on transfers of personal data apply when *personal data* is transferred or is accessed from outside the EEA, including when this is done for training AI systems, and in the phase of fine-tuning or cross-border application of already existing AI systems located outside the EEA to individuals located in the EEA.[41] This is because feeding an EEA individual's data to the non-EEA AI system will most likely constitute a transfer of personal data.

Turning to the intersection of the GDPR with international trade law, only one FTA to which the EU is a party includes a binding provision on cross-border data flows. The 2019 Economic Partnership Agreement with Japan (Japan–EU EPA), where such a provision was initially proposed by Japan, merely includes a review clause allowing the parties to revisit the issue in three years' time after the agreement's entry into force.[42] The EU and Japan have agreed to use a mutual adequacy decision following the route for cross-border transfers of personal data laid down in the GDPR.[43] This was due to the inability of EU institutions to reach a common position on the breadth of the data flows provision and exceptions from it for the protection of privacy and personal data, following a strong push back from academics and civil society to an attempt of including such provisions in the –

[38] Article 2(2) Regulation 2018/1807 of the European Parliament and of the Council on a Framework for the Free Flow of Non-personal Data in the European Union, OJ L [2018] 303/59, 28 November 2018 [hereinafter: EU Regulation 2018/1807]; European Commission, Guidance on the Regulation on a Framework for the Free Flow of Non-personal Data in the European Union, COM(2019) 250 final, 29 May 2019, at para. 2.2.

[39] EU Regulation 2018/1807, note 38, Recital 9.

[40] A. Chander and U. P. Lê, 'Breaking the Web: Data Localization vs. the Global Internet', UC Davis Legal Studies Research Paper No 378, at 40; A. Goldfarb and D. Trefler, 'AI and International Trade', NBER Working Paper No 24254 (2018), at 20–22.

[41] The notion of 'transfer' of personal data is not clearly defined in the GDPR or in the guidance of the Data Protection Authorities. It can indirectly be implied from the existing guidance on the mechanisms for transfers of personal data that a 'transfer' is understood broadly, as it also captures continuous cross-border access to EEA personal data from abroad. See European Data Protection Board, Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679, 25 May 2018.

[42] Article 8.81 of EU–Japan EPA. The same provision is also included in Article XX chapter 16 of draft EU–Mexico FTA, negotiated roughly at the same time as the EU–Japan EPA. See also B. Fortnam, 'EU Punts on Data Flow Language in Japan Deal, Leaving Position Unresolved', *Inside US Trade*, 7 June 2017.

[43] European Commission, 'European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows', *Press Release*, 23 January 201.

currently stalled – plurilateral Trade in Services Agreement (TiSA) and the Transatlantic Trade and Investment Partnership (TTIP) between the EU and the US.[44]

In 2018, the European Commission reached a political agreement on the EU position on cross-border data flows. This position was expressed in the model clauses, which, in particular, include a model provision on cross-border data flows (Article A) and an exception for the protection of privacy and personal data (Article B).[45] The EU has included these model clauses in its proposals for digital trade chapters in the currently negotiated trade agreements with Australia, Indonesia, New Zealand and Tunisia,[46] as well as into the EU proposal for the WTO rules on electronic commerce,[47] which are intended to co-exist with the general exception for privacy and data protection modelled after Article XIV(c)(ii) GATS included in the same agreements.[48] The 2021 EU-UK Trade and Cooperation Agreement (TCA), however, contains provisions different and, arguably, awarding less regulatory autonomy to protect privacy and personal data, than those in the

[44] K. Irion, S. Yakovleva, and M. Bartl, *Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements* (Amsterdam: Institute for Information Law, 2016), at 44–45, 59–60; M. Fernández Pérez, 'Corporarivacy Confusion in the EU on Trade and Data Protection', *EDRi*, 12 October 2016; European Parliament, Resolution of 8 July 2015 Containing the European Parliament's Recommendations to the European Commission on the Negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228 (INI)); European Parliament, Resolution of 3 February 2016 Containing the European Parliament's Recommendations to the Commission on the Negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI)).

[45] European Commission, Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements, February 2018, available at https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[46] European Commission, EU's Proposal for the Digital Trade Chapter of EU–New Zealand FTA, 25 September 2018 [hereinafter: EU Proposal Digital Trade Chapter EU–New Zealand FTA], available at http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157581.pdf; European Commission, EU's Proposal for the Digital Trade Chapter of EU–Australia FTA, 10 October 2018 [hereinafter: EU Proposal Digital Trade Chapter EU–Australia FTA], available at http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf; European Commission, EU's Proposal for the Digital Trade Chapter of EU–Tunisia FTA, 9 November 2018, available at https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157660.%20ALECA%202019%20-%20texte%20commerce%20numerique.pdf; European Commission, Report of the 5th Round of Negotiations for a Free Trade Agreement between the European Union and Indonesia, 9–13 July 2018, Brussels, available at http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157137.pdf. The EU's Proposal for Digital Trade Chapter for a Modernised EU–Chile Association Agreement only contains a placeholder for provisions on data flows (see EU–Chile FTA, 5 February 2018, available at https://trade.ec.europa.eu/doclib/docs/2018/february/tradoc_156582.pdf).

[47] WTO, Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, Communication from the European Union, INF/ECOM/22, 26 April 2019 [hereinafter: EU Proposal Joint Statement Initiative].

[48] See, e.g., Article X.1(2) of the EU proposal for Chapter X, 'Exceptions' of the EU–New Zealand FTA, 25 June 2019, available at https://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158278.pdf [hereinafter: Proposal for Exceptions]. This provision includes a general exception for privacy and data protection modelled after the general exception in Article XIV(c)(ii) GATS. EU proposals for 'Exceptions' chapters of other FTAs discussed in this chapter are not available as of the time of writing.

above-mentioned model clauses.[49] It is unclear whether the TCA provisions are merely outliers or represent the new model approach of the EU. Given that the above-mentioned model clauses have not been amended following the TCA and still represent the EU position in multiple ongoing trade negotiations, including those at the WTO, this chapter assumes that they still represent the EU mainstream approach and, therefore, the discussion below focuses solely on these clauses.

Model Article A provides for an exhaustive list of prohibited restrictions on cross-border data flows. Model Article B on the *protection of personal data and privacy* states that the protection of personal data and privacy *is a fundamental right* and includes an exception from the provision on cross-border data flows. The model clauses, on their face, safeguard the EU's broad regulatory autonomy, much more so than the general exception for privacy and data protection in existing trade agreements. This is made manifest in five different ways. First, as compared to the US model provision on cross-border data flows, the prohibition of restrictions on cross-border data flows in Article A is formulated more narrowly, in that it specifically names the types of restrictions that are outlawed by this provision. Second, the provisions of Article B(1) assert that the normative rationale for the protection of personal data and privacy is the protection of fundamental rights. This rationale – as opposed to economic reasons for protecting privacy and personal data – signals a higher level of protection and, therefore, arguably requires a broader autonomy to regulate vis-à-vis international trade commitments.[50] This provision is likely to be interpreted as a part of the digital trade exception for privacy and data protection in Article B(2) of the proposal. Third, the proposed exception for privacy and the protection of personal data establishes a significantly more lenient threshold – 'it deems appropriate' – than the 'necessity test' of the general exception under the GATS. Drawing the parallel with the threshold in the GATS national security exception – 'it considers necessary'[51] – one can argue that the proposed exception affords an almost unlimited autonomy to adopt measures inconsistent with Article B (2) to protection of privacy and personal data.[52] Fourth, the exception in Article B(2) explicitly recognises the adoption and application of rules for cross-border transfers of personal data – the gist of the EU's framework for transfers of personal data – as one of the measures that a party may deem appropriate to protect personal data and privacy, in spite of its international trade commitments. Fifth and finally, the

[49] Articles DIGIT. 6 and DIGIT. 7 of the TCA; for a critical assessment from a data protection perspective, see Opinion 3/2021 of the European Data Protection Supervisor on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement.

[50] For argumentation on this point, see Yakovleva, note 16, at 507–511.

[51] Article XIV *bis* GATS.

[52] The national security exception is the broadest of all the existing exceptions in international trade law. It is for this reason that it was labelled as 'all-embracing and seemingly omnipotent'. See J. Yeong Yoo and D. Ahn, 'Security Exceptions in the WTO System: Bridge or Bottle-Neck for Trade and Security?', *Journal of International Economic Law* 19 (2016), 417–444, at 426.

provision of Article B(2) protects the safeguards afforded by a party for personal data and privacy from being affected by any other provision of the trade agreement.

At the same time, despite these apparent strengths of the EU proposal in view of privacy and data protection, Article B suffers from at least four clear weaknesses. First, declaring that the protection of privacy and personal data are fundamental rights is EU-centric and does not leave the EU's trading partners any autonomy to choose another level of protection of these public policy interests they might see fit for their own legal and cultural tradition. Given that, as things stand now at least, the fundamental rights protection of privacy and personal data is, essentially, a European phenomenon, EU trading partners may be reluctant to commit to this level of protection in a trade agreement. Second, the exception for privacy and data protection in Article B(2) of the EU's proposal is designed for digital trade chapters and fails to clarify its relationship with the general exception for data protection, which remains intact – at least in available draft trade agreements – in which the EU has included the proposed model clauses.[53] Third, modelling an exception for privacy and data protection after the national security exception essentially creates an almost unconditional escape valve from virtually any trade commitment, as long as there is at least a remote nexus to the protection of privacy and personal data. Although this may seem justified at first glance given that privacy and data protection are fundamental rights in the EU, it creates a precedent for using this wide margin for a variety of public policy interests (other than national security), which may undermine the global rules-based trading system. Fourth, and most relevant in the context of this chapter's discussion, the public policy interests that can justify violation of Article A under Article B(2) are limited to the protection of privacy and personal data. Although this underscores the relative importance of the rights to data protection and privacy as opposed to the goal of digital trade liberalisation on the values scale, the limitation of the exception to these particular rights may have negative effects. Given that the threshold for important public policy interests, such as public morals, safety, human, animal or plant life, in the general exception clause is narrower than the threshold in model Article B(2), the regulatory autonomy to protect personal data and privacy ends up being much broader than the protection of other rights that are also recognised under the EU Charter of Fundamental Rights.[54] This elevates privacy and the protection of personal data above other rights that are equally protected[55] and may even create an incentive to – artificially – frame other public policy interests, especially those not mentioned in the GATS general exception, as protection of privacy and personal data. In the context of AI, this could steer domestic AI regulation in the EU deeper into the realm of data protection as

[53] Proposal for Exceptions, note 48.

[54] See, for example, Articles 2 (right to life), 6 (right to liberty and security), 37 (environmental protection) EU Charter of Fundamental Rights.

[55] K. Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights', *European Constitutional Law Review* 8 (2012), 375–403, at 392–393.

opposed to creating a separate regulatory framework – an issue currently discussed in the EU institutions.[56] Public policy interests, such as industrial policy,[57] cybersecurity[58] and digital sovereignty,[59] are cited as public policy interests that may require restricting digital trade in general or data flows in particular. The first is especially relevant for developing countries, for which free data flows essentially mean 'one-way flows', as these countries' data flows are constrained by the limited availability of digital technologies and of the skills necessary to produce digital intelligence from data.[60] This issue, as already mentioned, has gained prominence in the European Commission's 2020 digital strategy. In its European Strategy for Data, the European Commission stated:

> The functioning of the European data space will depend on the capacity of the EU to invest in next-generation technologies and infrastructures as well as in digital competences like data literacy. This in turn will increase *Europe's technological sovereignty* in key enabling technologies and infrastructures for the data economy. The infrastructures should support the creation of European data pools enabling Big Data analytics and machine learning, in a manner compliant with data protection legislation and competition law, allowing the emergence of data-driven ecosystems.[61]

Turning to cybersecurity interests, they may require restrictions on data flows, data localisation or restrictions on import of certain information technology products.[62] These interests are relevant for both developing and developed countries. The blurring boundary between public and private spheres in the surveillance context – where governments increasingly rely on private actors for access to data for surveillance purposes – explains why cross-border data flows may raise sovereignty concerns as well.[63]

To sum up, although the regulation of cross-border data flows, especially in the context of AI, implicates a variety of public policy interests, the EU trade policy on this topic has solely focused on one of them – namely privacy and the protection of personal data. This,

[56] Compare White Paper on Artificial Intelligence (note 15) with EDPB Response to the MEP Sophie in't Veld's Letter on Unfair Algorithms, 29 January 2020, available at https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-mep-sophie-int-velds-letter-unfair-algorithms_en.

[57] C. Foster and S. Azmeh, 'Latecomer Economies and National Digital Policy: An Industrial Policy Perspective', *The Journal of Development Studies* 56 (2020), 1–17.

[58] Mitchell and Mishra, note 19, at 1079.

[59] See European Commission, A New Industrial Strategy for Europe, COM(2020) 102 final, 10 March 2020; White Paper on Artificial Intelligence, note 15. See also K. Propp, 'Waving the Flag of Digital Sovereignty', Atlantic Council, 11 December 2019.

[60] UNCTAD, note 1, at 91.

[61] European Commission, A European Strategy For Data, COM (2020) 66 final, 19 February 2020, at 5 (emphasis added).

[62] J. P. Meltzer and C. F. Kerry, 'Cybersecurity and Digital Trade: Getting It Right', Brookings, 18 September 2019.

[63] R. D. Williams, 'Reflections on TikTok and Data Privacy as National Security', Lawfare, 15 November 2019.

arguably, has something to do with the institutional dynamics between EU institutions. However, it may not be sustainable either in the EU or in a multilateral context, such as with regard to the electronic commerce negotiations at the WTO. According to UNCTAD, the early meetings of the group on data flows at the WTO have, so far, mainly reflected the views of proponents of the free flow of data.[64] However, for these negotiations to result in concrete WTO legal norms, members will have to reach a consensus on how to balance the economic gains of free data flows with multiple competing interests, which include not only the protection of privacy and personal data – the main point of contention for the EU – but also other fundamental rights, as well as industrial policy, cybersecurity and economic development interests of other countries involved in the negotiations.[65]

In contrast to the position taken both by the United States and the EU that data flows should be free (unless their restriction can be justified by an exception), when it comes to the protection of the source code, or algorithms expressed in that source code incorporating the *learning* derived from processing of data – the position is the exact opposite. As explained in the introduction, learning, or digital intelligence, is where the real economic value of personal and other data lies. Thus, while data and data flows are viewed as 'free', the value obtained from data are up for grabs by whomever possesses the infrastructure and resources necessary to process that data. At this juncture, these entities are concentrated in the United States and China. Two recent US-led FTAs, namely the USMCA and the US–Japan Digital Trade Agreement (DTA), contain specific provisions on the protection of source code and algorithms.[66] The EU's proposal for the WTO negotiations on e-commerce also contains a prohibition on access to and forced transfer of the source code of software owned by a natural or juridical person of other members.[67] Similar provisions are included in the EU proposals for digital trade chapters of currently negotiated FTAs, such as with Mexico,[68] Australia[69] and New Zealand.[70]

C THE LIMITS OF PERSONAL DATA PROTECTION IN THE CONTEXT OF TRADE LAW POLICY ON CROSS-BORDER DATA FLOWS IN AI CONTEXT

The earlier discussion demonstrates that the only public policy interests that are fully accounted for in the exception from a proposed provision on the free cross-border flow of data in draft EU trade agreements are privacy and the protection of personal data. In

[64] UNCTAD, note 1, at 137.
[65] S. Yakovleva and K. Irion, 'Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation', *AJIL Unbound* 114 (2020), 10–14, at 14.
[66] Article 19.16 USMCA; Article 17 US–Japan DTA.
[67] EU Proposal Joint Statement Initiative, note 47, at para. 2.6.
[68] Article 9 of the draft EU–Mexico FTA.
[69] Article 11 EU Proposal Digital Trade Chapter EU–Australia FTA.
[70] Article 11 EU Proposal Digital Trade Chapter EU–New Zealand FTA.

the context of AI, this mirrors the currently prevailing approach in the EU to regulate AI through the governance structure of the GDPR. This section focuses on two limitations of this approach. First, this approach is based on a distinction between personal and non-personal data, because only data that qualifies as personal falls under the EU data protection framework. The distinction is increasingly hard to make, especially in the context of AI. Second, EU privacy and personal data protection takes us to an individual rights framework that does not account for the value produced from data and the impact of applying the learning derived from AI to larger societal groups or populations.

I *Thin Borderline between Personal and Non-personal Data in AI Context*

EU law maintains a rigid distinction between personal and non-personal data,[71] in the sense that there are two different legal frameworks for personal and non-personal data. While cross-border transfers of personal data are subject to a 'border control'[72] regime, as discussed earlier, transfers of non-personal data outside the EEA are unrestricted. This distinction is increasingly unworkable in practice as it is becoming ever more difficult to draw a line between personal and non-personal (or anonymous) data, especially in the AI context.[73]

Schwartz and Solove succinctly summarise four main problems with the distinction. First, 'built-in identifiability' in cyberspace makes anonymity online a 'myth', as essentially all online data can be linked to some identifier.[74] Second, non-personal information can be transformed into personal data over time.[75] Third, the distinction between personal and non-personal data has a dynamic nature, as the line between the two depends on technological developments. Fourth and finally, the borderline between personal and non-personal data is not firm, but rather contextual, as many types of data are not non-identifiable or identifiable in the abstract.[76]

The EU regulation on a framework for the flow of non-personal data illustrates a number of those points. It specifically mentions that examples of non-personal data include 'aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and

[71] B.-J. Koops, 'The Trouble with European Data Protection Law', *International Data Privacy Law* 4 (2014), 250–261, at 257.

[72] D. J. B. Svantesson, 'The Regulation of Cross-Border Data Flows', *International Data Privacy Law* 1 (2011), 180–198, at 184.

[73] See, e.g., O. Tene and J. Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics', *Northwestern Journal of Technology and Intellectual Property* 11 (2013), 239–273; N. Purtova, 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law', *Law, Innovation and Technology* 10 (2018), 40–81; P. Ohm, 'Broken Promises of Privacy', *UCLA Law Review* 57 (2010), 1701–1777.

[74] P. M. Schwartz and D. J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', *New York University Law Review* 86 (2011), 1814–1894, at 1836–1848.

[75] Ibid.

[76] Ibid.

water, or data on maintenance needs for industrial machines'.[77] The regulation also notes, however, that '[i]f technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data, and [the GDPR] is to apply accordingly'.[78] As can be seen, although *the very existence of this regulation is grounded on the possibility of separating the notions of personal and non-personal data*, the regulation itself suggests that such distinction is not clear-cut and requires constant reassessment.

Another limitation of a data protection approach to restrictions on cross-border data flows in the AI context is that its scope is limited to data that qualifies as personal data. However, it is not the data fed into an AI system itself, but the *knowledge* derived from the data through *learning* that integrates the value of big data into different organisational processes. Training of AI systems transforms personal data into an aggregate representation of such data, which may no longer qualify as personal data. Interestingly, some scholars have argued in this context that AI models vulnerable to inversion attacks can still be considered personal data.[79] Moreover, it is not only personal, but also non-personal – machine-generated – data that is extremely useful and valuable in AI context. As the European Commission rightly noted in its 2020 White Paper on AI:

> AI is one of the most important applications of the data economy. Today most data are related to consumers and are stored and processed on central cloud-based infrastructure. By contrast a large share of tomorrow's far more abundant data will come from industry, business and the public sector, and will be stored on a variety of systems, notably on computing devices working at the edge of the network.[80]

Although cross-border flows of non-personal data and learning produced from it may not have implications for individual rights to privacy and the protection of personal data, they may present risks for other policy objectives, such as cybersecurity or digital sovereignty. The argument in this chapter is not to suggest that cross-border flows of non-personal data should be restricted, although a possibility of such restrictions already features in the European Commission's proposal for a Data Governance Act.[81] Neither does it suggest that a strong exception for domestic privacy and data protection rules is inappropriate. Rather, it underscores the importance of assessing the implications of cross-border data flows in the context of AI against a broader set of public policy interests that matter for the EU and its trading partners in the long term. For example, Gürses and van Hoboken are doubtful that,

[77] EU Regulation 2018/1807, note 38, at Recital 9.
[78] Ibid.
[79] M. Veale, R. Binns, and L. Edwards, 'Algorithms That Remember: Model Inversion Attacks and Data Protection Law', *Philosophical Transactions of the Royal Society* A 376 (2018), 1–15.
[80] White Paper on Artificial Intelligence, note 15, at 1.
[81] See, e.g., Articles 5, 30 of the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM/2020/767 final.

in the context of digital services produced in an agile way where users also act as producers of such services, privacy law, traditionally centred around regulating information flows, is able to tackle the implications for individuals of such agile production.[82] They argue that such problems should not all be framed as questions of information flows and data protection, but instead addressed by other, or complementary regulatory tools, such as consumer protection, software regulation or treatment of certain services as new types of utility providers.[83]

II *Individual Rights Framework Does Not Factor in the Value of Knowledge Derived from Data*

In the digital trade discourse where unrestricted cross-border data flows are viewed as a source of tremendous – *aggregated* – value gains, not every country participating in data flows 'wins' from those data flows. Yet, the issue of who wins and who loses from unrestricted data flows is typically not raised in this discourse. As mentioned earlier, only countries that possess the necessary infrastructure and skills to refine data and extract value from large corpora of data generated in the course of the provision of online services will really benefit from the free flow of data. As a result, countries that lack these resources are merely supplying primary goods, which are worth much less than the learning that can be derived from them, just as countries that produce raw materials are rarely the largest winners when compared to countries where those materials are transformed. Just as the real value lies in the transformation of raw materials, the real value in AI lies in the value of processing the data. Against this backdrop, focusing on data instead of learning derived from data misses the point.

This brings us to the second limitation of the data protection framework being central in cross-border provision of AI, especially in the way it is designed in the EU, where personal data is primarily viewed as the subject matter of a fundamental right rather than an economic asset. This is manifested, for example, in regulatory choices that avoided recognising personal data as consideration for online services (in other words, as a form of currency) in the 2019 Digital Content Directive.[84] In its opinion on the draft of this directive, the European Data Protection Supervisor (EDPS) underscored that 'personal data cannot be *considered as a mere commodity*'.[85] Although the fact that the personal data cannot be considered as a 'mere'

[82] S. Gürses and J. van Hoboken, 'Privacy after the Agile Turn', in E. Selinger, J. Polonetsky, and O. Tene (eds), *The Cambridge Handbook of Consumer Privacy* (Cambridge: Cambridge University Press, 2018), 597–601.

[83] Ibid.

[84] Directive 2019/770 of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services, OJ L [2019] 136/1, 22 May 2019. For discussion, see European Data Protection Supervisor (EDPS), Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content, 14 March 2017.

[85] Ibid., at 3 (emphasis added).

commodity does not mean that it cannot have economic value, viewing the protection of personal data as a fundamental right could be one of the reasons why the EU could be restrained in putting a price tag on personal data in trade negotiations on cross-border data flows.

UNCTAD stresses that platforms harnessing data generated by individuals, businesses and organisations of other countries, while based in only a few countries, raises concerns about 'digital sovereignty', in view of the control, access and rights with respect to the data and the appropriation of the value generated from monetising the data.[86] UNCTAD explains that economic value derived from data is captured by developed countries where companies having control over storage and processing of data reside.[87] It follows, that '[t]he only way for developing countries to exercise effective economic "ownership" of and control over the data generated in their territories may be *to restrict cross-border flows of important personal and community data*'.[88] Although this particular report makes an argument in the context of imbalance between developed and developing countries, given the high concentration of digital technologies in the very few developed countries, it could also be relevant in relations between those few and other developed countries. It should be emphasised that restricting the outgoing flows of personal data does not mean that those countries that impose such restrictions will have the means to process and generate value from such data within their borders. It may be about sovereignty, but it is not necessarily about endogenous economic development unless measures to ensure this development accompany the data flow restrictions.

In a similar vein, Couldry and Mejias speak about 'data colonialism', by which they mean that big data processing practices make human relations and social life overall 'an "open" resource for extraction'.[89] They compare big data to appropriation or extraction of resources[90] – another parallel between data and oil. Global data flows, they argue, 'are as expansive as historic colonialism's appropriation of land, resources, and bodies, although the epicentre has somewhat shifted'.[91] In their view, the transformation of human actors and social relations formalised as data into value leads to a fundamental power imbalance (colonial power and colonised subjects).[92] In a similar vein, Zuboff has famously labelled the business of accumulation and

[86] UNCTAD, note 1, at 89.
[87] Ibid.
[88] Ibid. (emphasis added).
[89] N. Couldry and U. A. Mejias, 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject', *Television and New Media* 20 (2019), 336–349, at 337.
[90] Ibid., at 338.
[91] Ibid., but see M. Mueller and K. Grindal, 'Data Flows and the Digital Economy: Information as a Mobile Factor of Production', *Digital Policy, Regulation and Governance* 21 (2019), 71–87, at 82, challenging this point of view.
[92] Couldry and Mejias, note 87, at 337–338.

monetising data 'surveillance capitalism', which leads not only to the accumulation of capital, but also of individual rights.[93]

There is some movement in the governance of data reflecting those concerns. A 2019 Opinion of the German Ethics Commission shows a tendency towards expanding the scope of individual rights in data beyond the non-economic rights to privacy and personal data protection. According to the commission, under certain circumstances individuals should be granted data-specific rights, which include a right to obtain an economic share in profits derived with the help of the data.[94] The potential design of a *legal framework of distribution* of economic gains from the use of data is addressed in a growing body of scholarly and policy research. This research explores frameworks or organisations acting as intermediaries between individuals and entities wishing to use (and profit from) their data, such as *data trusts* or collective data ownership (such as data funds).[95] Data trusts are viewed as an attractive tool to facilitate access to large data sets of aggregated data for the purposes of developing and applying AI, to generate trust around the use of data by various stakeholders, and as mechanisms for paying back a fair share of benefits from the use of data to individuals.[96] There is, however, little clarity regarding the structure that data trusts should take and the method for sharing value derived from the commercial use of personal data.[97] The German Ministry of Economic Affairs and the Dutch Government are investigating the possibilities of setting up data trusts in their respective countries.[98] Research on data funds views personal data as a *public resource*, drawing a parallel with natural resources that constitute the country's resource. From this perspective, data collected within a certain jurisdiction should 'belong' to that jurisdiction.[99] Data funds are viewed as a form of collective data ownership, allowing individuals to exercise control over which data is collected about them and how it is used, as well as to receive payment for commercial access to the data in the fund.[100]

[93] S. Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization', *Journal of Information Technology* 30 (2015), 75–89.

[94] German Data Ethics Commission, *Opinion of the Data Ethics Commission: Executive Summary* (Berlin: Data Ethics Commission of the Federal Government, 2019), at 9–10.

[95] For an overview, see UNCTAD, note 1, at 132–134.

[96] J. Hardinges, 'What Is a Data Trust? What's the Definition and How Is One Applied?', Open Data Institute, 10 July 2018; S. Delacroix and N. D. Lawrence, 'Bottom-Up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance', *International Data Privacy Law* 9 (2019), 236–252; W. Hall and J. Pesenti, *Growing the Artificial Intelligence Industry in the UK* (London: Government of the United Kingdom, 2017).

[97] Hall and Pesenti suggesting that the trusts should take a form of a repeatable framework. Ibid.

[98] Motie Buitenweg c.s. over vormgeving van data trusts in Nederland – Initiatief nota van het lid Verhoeven over mededinging in de digitale economie, Tweede Kamer der Staten-Generaal, 35134 nr. 7, 18 December 2019, available at: www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vl4jjboml8yr.

[99] UNCTAD, note 1, at 132.

[100] See, e.g., E. Morozov, 'To Tackle Google's Power, Regulators Have to Go after Its Ownership of Data', *The Guardian*, 2 July 2017.

These economic rights are unlikely to become a part of the EU data protection framework precisely due to their economic nature. At the same time, they could interfere with international trade disciplines which aim to facilitate the unrestricted cross-border data flows. This is why they should form part, in addition to the fundamental rights to protection of privacy and personal data, of a nuanced rebalancing of the EU's trade policy on this issue.

D CONCLUSION

The analysis in this chapter of recent developments in the governance of cross-border data flows in international trade law showed that the main public policy interests discussed in the context of EU trade policy on this issue are the protection of the fundamental rights to privacy and personal data. This chapter argued that other policy objectives, such as cybersecurity and digital sovereignty – which have recently become one of the anchors of EU's internal AI policy – should also be considered. The chapter has also shown that the individual rights–centred data protection framework has limits in governing AI both in domestic and international trade policy.