

Panta Rhei

A European Perspective on Ensuring a High Level of Protection of Human Rights in a World in Which Everything Flows

Kristina Irion*

A INTRODUCTION

Pantha rhei ('everything flows') turns out to be a very fitting metaphor for how terabytes of digital data rush through the network of networks. Attributed to the philosopher Heraclitus *panta rhei* connotes that change is the fundamental essence of the universe.¹ Data flows are the undercurrent of digital globalization that transforms our societies. How data flows will likely underpin digital services in a not so distant future is vividly described in Anupam Chander's contribution (Chapter 5) in this volume. Data's liquidity tends to undermine outdated regulatory formations and erode the paradigms that used to underpin a society's conventional right to self-governance.² Everything is in flux.

Human rights do however remain valid currency in how we approach planetary-scale computation and accompanying data flows. As we enter 'the age of digital interdependence', a UN expert panel urges 'new forms of digital cooperation to ensure that digital technologies are built on a foundation of respect for human rights and provide meaningful opportunity for all people and nations'.³ Today's system of human rights protection, however, is highly dependent on domestic legal

* Kristina Irion is Associate Professor at the Institute for Information Law (IViR), University of Amsterdam. I would like to enthusiastically thank Dr Mira Burri and her team as well as the participants of the conference 'Big Data and Global Trade Law', 16–17 November 2018, Lucerne, Switzerland. Contact: k.irion@uva.nl.

¹ Actually, it is Plato's interpretation based on an aphorism from the Heraclitean River Fragments that reads in English translation, 'On those stepping into rivers staying the same, other and other waters flow'. See D. W. Graham, 'Heraclitus: Flux, Order, and Knowledge', in P. Curd and D. W. Graham (eds), *The Oxford Handbook of Presocratic Philosophy*, Vol. 1 (Oxford: Oxford University Press, 2009), 167–188.

² J. E. Cohen, *Between Truth and Power* (Oxford: Oxford University Press, 2019), at 200.

³ United Nations Secretary-General's High-Level Panel on Digital Cooperation, *Report of the UN Secretary-General's High-Level Panel on Digital Cooperation: The Age of Digital Interdependence* (New York/Geneva: United Nations Publications, 2019).

institutions, which unravel faster than the reconstruction of fitting transnational governance institutions. The transnational protection of data privacy is a case in point, which required legal reforms in order not to fall into the cracks between different domestic legal systems. Furthermore, the transnational provision of artificial intelligence (AI) is going to have a bearing on the conditions of human freedom prompting calls for a human rights-based approach to AI governance.⁴

Through the contribution in this volume it emerges that international trade law has successfully co-opted cross-border data flows as a desirable baseline for digital trade. This raises the question how the inclusion of the free flow of data in international trade law would affect the prospects for the transnational protection of human rights. As a stand-alone commitment, the free flow of data namely lacks any normative underpinning and only through the interplay with domestic legal frameworks do human rights become recognized.

In my contribution I argue that the inclusion of cross-border data flows as a new trade law discipline would be opportunistic in light of the morality to protect human rights online. International trade law, which has been criticized for the ‘economization of human rights’,⁵ would subtly reinforce the transformative power of data flows leaving human rights enforcement to domestic institutions which in themselves have been found inferior to deal with the issues at hand. In other words, the opportunity structures offered by international trade law will not advance the construction of a global information civilization that is founded on the respect for human rights. Rather, multilevel economic governance should provide for constitutional pluralism and sufficient margin for experimentation with novel strategies to give effect to human rights in the online context.⁶ I conclude with a plaidoyer for a new quid pro quo in digital trade in which the liberalization of cross-border data flows recognizes better the enhanced need for human rights accountability. This contribution intersects human rights law with international economic law, liberally borrowing from transnational legal theory and Internet governance literature. It advances its arguments through a combination of doctrinal and critical legal research with a certain predisposition to European legal thinking.

This chapter proceeds as follows: after the backdrop has been set, the following section takes a critical look at the construction of the data flow metaphor as a policy concept inside international trade law. The subsequent section explores how the respect for human rights ties in with national constitutionalism that becomes increasingly challenged by the transnational dynamic of digital era transactions.

⁴ N. A. Smuha, ‘Beyond a Human Rights-Based Approach to AI Governance: Promise, Pitfalls, Plea’, *Philosophy and Technology* (2020).

⁵ C. Breining-Kaufmann, ‘The Legal Matrix of Human Rights and Trade Law: State Obligations versus Private Rights and Obligations’, in T. Cottier, J. Pauwelyn, and E. Bürgi (eds), *Human Rights and International Trade* (Oxford: Oxford University Press, 2005), 95–136, at 104.

⁶ E.-U. Petersmann, ‘Need for a New Philosophy of International Economic Law and Adjudication’, *Journal of International Economic Law* 17 (2014), 639–669, at 663.

The last section turns to international trade law and why its ambitions to govern cross-border data flows will likely not advance efforts to generate respect for human rights. In the conclusion, the different arguments are linked together to advocate for a re-balancing act that recognizes human rights inside international trade law.

B DATA FLOW AS A POLICY METAPHOR

Data is the building block of today's digital economy. As a virtual unit data can represent any type of digital infrastructure, platform, or system, that undergird an infinite range of virtual goods, services, transactions and expressions. Digital supply and value chains are ultimately representations of data which are assembled to perform varying functionalities.⁷ Besides data is exponentially generated from any human and machine activity, which in turn are a key input for machine learning and algorithmic decision-making. Everything that can be expressed in data is inherently liquid because it can be de-assembled, moved across space and re-assembled again.

In social theory 'flow', 'fluidity' or 'liquidity' are used as a metaphor to connote how circulation and velocity forge a new kind of information or network society.⁸ According to Castells, contemporary society is constructed around flows: 'flows of capital, flows of information, flows of technology, flows of organizational interaction, flows of images, sounds, and symbols. Flows are not just one element of the social organization: they are the expression of processes dominating our economic, political, and symbolic life'.⁹ Sociologist Deborah Lupton, by contrast, criticizes that writers on digital technologies rely on liquid concepts when discussing the circulation of digital data.¹⁰ For Lupton, '[t]he apparent liquidity of data, its tendency to flow freely, can also constitute its threatening aspect, its potential to create chaos and loss of control'.¹¹ Lupton nevertheless resolves that such conceptions can help making sense of the phenomenon. It must be conceded that the recourse to the data flow metaphor should not divert from analyzing actors, the epistemology and affordances of concrete sociotechnical systems.¹² Globalization researchers, however, consistently use the cross-border movement or flows of

⁷ Instructive on this: B. H. Bratton, *The Stack: On Software and Sovereignty* (Cambridge, MA: MIT Press, 2015).

⁸ T. Sutherland, 'Liquid Networks and the Metaphysics of Flux: Ontologies of Flow in an Age of Speed and Mobility', *Theory, Culture and Society* 30 (2013), 3–23.

⁹ M. Castells, *The Rise of the Network Society*, 2nd edn (Oxford: Blackwell, 2010), at 442.

¹⁰ D. Lupton, *Digital Sociology* (Abingdon: Routledge, 2014), at 106.

¹¹ *Ibid.*

¹² See, e.g., B. Bodo et al., 'Tackling the Algorithmic Control Crisis – The Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents', *Yale Journal of Law and Technology* 19 (2017), 133–180; J.-C. Plantin et al., 'Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook', *New Media and Society* 20 (2018), 293–310; A. Helmond, *The Web as Platform* (PhD thesis, University of Amsterdam, 2015).

persons, capital, goods and services as a conceptual lens, which is currently complemented by data flows. It is precisely the circulation of data which underpins the processes that lead to the reconfiguration of the spatial organization of social relations and transactions that characterize globalization.¹³ A 2016 report by the McKinsey Global Institute proclaimed that globalization had entered ‘a new era defined by data flows’.¹⁴

A powerful coalition of international and intergovernmental organizations, including the G7 and the G20, the Organisation for Economic Cooperation and Development (OECD) and the World Economic Forum (WEF), among others, have intensified their work on promoting cross-border data flows as an international economic policy principle. For instance, following the initiative of Japan’s government on ‘Data Free Flow with Trust’, the 2019 G20 Osaka Leaders’ Declaration states:

Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security. By continuing to address these challenges, we can further facilitate data free flow and strengthen consumer and business trust. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected. Such data free flow with trust will harness the opportunities of the digital economy.¹⁵

While the statement correctly reflects the unabated tension between cross-border data flows and domestic legal frameworks, it falls short of identifying common strategies that would mitigate this tension and thereby forging trust in legitimate cross-border data flows. The endorsement of ‘Data Free Flow with Trust’ perfectly encapsulates the influential narrative of innovation, growth and development associated with cross-border data flow while leaving the intricacies of protecting human rights and societal values to domestic institutions that are themselves increasingly contested in an interdependent world. From the perspective of domestic public policy, the cross-border flow of data more fittingly compares to a maelstrom that potentially erodes constitutionally guaranteed rights and societal values.

C HUMAN RIGHTS DO NOT FLOW EASILY ACROSS BORDERS

Adopted over seventy years ago, the Universal Declaration of Human Rights (UDHR) protects a canon of universal and indivisible human rights the

¹³ D. Held et al., *Global Transformations: Politics, Economics, and Culture* (Stanford: Stanford University Press, 1999), at 16.

¹⁴ J. Manyika et al., *Digital Globalization: The New Era of Global Flows* (Washington, DC: McKinsey Global Institute, 2016).

¹⁵ G20, ‘G20 Osaka Leaders’ Declaration’, 2020, available at www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf, at para. 11.

interpretation of which evolves with the time.¹⁶ Already twice the UN Human Rights Council has affirmed that human rights must be protected offline and online regardless of frontiers.¹⁷ International human rights law is addressed to states which are bound to respect and uphold the obligations in their domestic legal system. Whereas international human rights law can take different levels of commitment from non-binding to binding, its enforcement overwhelmingly takes place at the domestic level.¹⁸ ‘The multilevel human rights constitution’, as Ernst-Ulrich Petersmann explains, ‘remains embedded into national constitutionalism as protected by national and regional courts’.¹⁹ Human rights thus wield universal protection from their geopolitically fragmented implementation by states. This construction has largely been workable in an offline and static world where different jurisdictions could coexist by the intuitive demarcations of territoriality. In the age of digital interdependence, however, interferences with human rights frequently take a transnational dynamic. According to Julie Cohen, domestic protections for human rights that are built on outdated regulatory formations have begun to fail comprehensively.²⁰ Different trends, such as the intermediation of human transactions by digital platforms, and strategies that would outsmart national legal frameworks have been held responsible for the sad state of affairs.²¹ From the outset the Internet-mediated sphere has attracted much libertarianism and utopianism,²² but in hindsight too little concern about the impeding policy and regulatory challenges online.

I *Who Should Be in Charge of the Internet?*

In its infancy the Internet has attracted utopian ideas of a free and borderless cyberspace, a human-made global commons in the service of an international community of users. Famously, John Perry Barlow in his ‘Declaration of the Independence of Cyberspace’ called on governments of the world to leave the

¹⁶ General Assembly of the United Nations, Universal Declaration of Human Rights, 3rd Session, A/RES/217(III), adopted 10 December 1948.

¹⁷ United Nations Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/RES/32/13, adopted on 18 July 2016; United Nations Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/38/L.10/Rev.1, adopted 4 July 2018.

¹⁸ One exception is the European Convention on Human Rights, which is enforceable through the European Court of Human Rights for state members of the Council of Europe.

¹⁹ Petersmann, note 6, at 644.

²⁰ Cohen, note 2, at 239.

²¹ Ibid.; J. van Dijck, T. Poell, and M. de Waal (eds), *The Platform Society* (Oxford: Oxford University Press, 2018).

²² F. Turner, *From Counterculture to Cyberculture* (Chicago: The University of Chicago Press, 2006); I. de Sola Pool, *Technologies of Freedom* (Cambridge, MA: Harvard University Press, 1983).

Internet and its users alone.²³ Another proposal was to transform cyberspace into an international commons and to root Internet governance in international agreements. Analogies to Hugo Grotius' 1609 dissertation 'Mare Liberum'²⁴ have been offered to extend a similar regime to the Internet as is practiced today in international maritime law and space law. Despite gigantic efforts to nourish international multi-stakeholder Internet governance up to this point, this approach has never gained sufficient authority to actually deliver tangible outcomes.²⁵ The upshot is that the protection of individuals' human rights online has never been uploaded to a supranational level.

Simultaneously, the Westphalian nation state that derives sovereignty and jurisdiction from territory has been contested as 'an ordering device for the borderless Internet'.²⁶ Cedric Ryngaert and Mark Zoetekouw are looking at 'community-based systems' as jurisdictional alternatives to territory which would better respond to the peculiar nature of the Internet as a 'borderless, prima facie, non-territorial phenomenon'.²⁷ Correspondingly, Francesca Bignami and Giorgio Resta expect that 'the social interactions fostered by borderless digital communications should give rise to a common set of moral commitments that will gradually replace those of the nation-state'.²⁸ It somewhat resonates with how large user-backed digital platforms frequently invoke their community in matters that affect platform governance.²⁹ Lee Bygrave highlights the peculiar contribution of contract law to manage large numbers of users across countries and legal systems via terms of service, for example.³⁰ Whereas transnational private law could achieve private platform governance from the inside, it does not compare to an external human rights-based governance framework.

²³ J. P. Barlow, 'A Declaration of the Independence of Cyberspace', 8 February 1996, available at <http://homes.eff.org/~barlow/Declaration-Final.html>.

²⁴ H. Grotius and R. van Deman Golphin, in J. Brown Scott (ed), *The Freedom of the Seas* (Oxford: Oxford University Press, 1916).

²⁵ See L. DeNardis, 'Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance', *Information Communication and Society* 15 (2012), 720–738; J. Hofmann, C. Katzenbach, and K. Gollatz, 'Between Coordination and Regulation: Finding the Governance in Internet Governance', *New Media and Society* 19 (2017), 1406–1423.

²⁶ F. Bignami and G. Resta, 'Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance', in E. Benvenisti and G. Nolte (eds), *Community Interests Across International Law* (Oxford: Oxford University Press, 2018), at 357.

²⁷ C. Ryngaert and M. Zoetekouw, 'The End of Territory? The Re-Emergence of Community as a Principle of Jurisdictional Order in the Internet Era', in U. Kohl (ed), *The Net and the Nation State: Multidisciplinary Perspectives on Internet* (Cambridge: Cambridge University Press, 2017).

²⁸ Bignami and Resta, note 26.

²⁹ R. MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York: Basic Books, 2012).

³⁰ L. A. Bygrave, *Internet Governance by Contract* (Oxford: Oxford University Press, 2015).

II Reactive Jurisdictional Claims

Legal thinking moreover diverges over the question whether online activities and Internet transactions should be treated as distinct from jurisdictional claims based on geographical location.³¹ To Hannah Buxbaum, conflicts about jurisdiction are a strategy where ‘claims of authority, or of resistance to authority’ are made by actors to advance a particular interest.³² The beneficiaries of a global reach for that matter reflexively push back jurisdictional claims from countries where the recipients of online service are based. Frequently technology-based arguments are invoked to deny the existence of a sufficient nexus for jurisdiction and the applicability of rules interdicting certain behaviour.³³ Joel Reidenberg intriguingly warns that this in turn would disable states from effectively protecting their citizens online.³⁴

Not being set in stone domestic legal institutions are reactive to the very context they are embedded in. The transnational protection of data privacy is a case in point to illustrate the crucial role of domestic legal frameworks in upholding human rights. When it became apparent that the regulation of domestic businesses no longer suffices to govern cross-border data transactions, legislators as well as courts resort to the external application of domestic laws. The European Union’s General Data Protection Regulation (GDPR)³⁵ is a prominent example for this legal technique that refocuses the territorial scope of application to organizations that are not established in the Union as long as they collect and use personal data of individuals who are inside the Union.³⁶ Likewise the California Consumer Privacy Act (CCPA) applies to businesses around the whole world as long as they reach out to California residents.³⁷ This is how after some backlog domestic legal institutions tweak jurisdictional concepts in their quest for asserting domestic rules which would still resonate with public international law.³⁸

³¹ Well recorded is the debate between the proponents of exceptionalism and its opponents, the non-exceptionalists, arguing over the source of authority that should regulate the Internet. See, e.g., D. R. Johnson and D. G. Post, ‘Law and Borders: The Rise of Law in Cyberspace’, *Stanford Law Review* 48 (1996), 1367–1402; J. Goldsmith and T. Wu, *Who Controls the Internet: Illusions of a Borderless World* (Oxford: Oxford University Press, 2006), for the opposing positions.

³² H. L. Buxbaum, ‘Territory, Territoriality, and the Resolution of Jurisdictional Conflict’, *American Journal of Comparative Law* 57 (2009), 631–675, at 635.

³³ *Ibid.*

³⁴ J. R. Reidenberg, ‘Technology and Internet Jurisdictions’, *University of Pennsylvania Law Review* 153 (2005), 1951–1974.

³⁵ 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, OJ L [2016] 119/1.

³⁶ M. Gömann, ‘The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement’, *Common Market Law Review* 54 (2017), 567–590; C. Ryngaert and M. Taylor, ‘The GDPR as Global Data Protection Regulation?’ *AJIL Unbound* 45 (2019), 5–9.

³⁷ The California Consumer Privacy Act of 2018, AB-375, 28 June 2018.

³⁸ For details, see Ryngaert and Taylor, note 36.

Predictably, such reactions are bound to run into an impasse about their effectiveness or legitimacy depending on from whose perspective one wishes to look at a particular issue. As a result, the international order now faces additional challenges, such as overlapping claims of authority and the transnational export of rules. Inquiries from the field of transnational data privacy also have shown that the extraterritorial reach of domestic rules may be overly formalistic and not matched with corresponding enforcement powers.³⁹ In their quest to overcome the enforcement fallacy domestic authorities are increasingly turning to governance by platforms deputizing ‘multinational corporate data intermediaries to carry out and enforce their orders’.⁴⁰ Yet, asserting domestic human rights regardless of jurisdiction, citizenship and location of data with the help of powerful digital platforms further entrenches the power of private economic interests over the conditions of human freedom.⁴¹

D INTERNATIONAL TRADE LAW LAYING CLAIM TO FREE DATA FLOWS

The flow of data crucially undergirds the organization of international production, trade and investments into global value chains (GVC).⁴² Activating international trade law for cross-border digital trade issues can be seen as ‘forum shopping in global governance’,⁴³ where trade venues are traditionally more conducive to economic interests than for that matter the multi-stakeholder Internet governance fora.⁴⁴ What is more, since trade rules on e-commerce could not advance under the auspices of the World Trade Organization (WTO), a number of countries have turned to preferential trade agreements instead, be they bilateral, regional or plurilateral.⁴⁵

³⁹ D. J. B. Svantesson, ‘The Regulation of Cross-Border Data Flows’, *International Data Privacy Law* 1 (2011), 180–198; C. Kuner, ‘Reality and Illusion in EU Data Transfer Regulation Post *Schrems*’, *German Law Journal* 18 (2017), 881–918.

⁴⁰ P. S. Berman, ‘Conflicts of Law and the Challenge of Transnational Data Flows’, in P. Zumbansen (ed), *The Many Lives of Transnational Law: Critical Engagements with Jessup’s Bold Proposal* (Cambridge: Cambridge University Press, 2020), 240–268.

⁴¹ J. Barry and E. Pollman, ‘Regulatory Entrepreneurship’, *Southern California Law Review* 90 (2016), 383–448; Cohen, note 2, at 329.

⁴² M. Burri, *Current and Emerging Trends in Disruptive Technologies: Implications for the Present and Future of EU’s Trade Policy* (Brussels: European Parliament, 2017), at 11; J. P. Meltzer, ‘Governing Digital Trade’, *World Trade Review* 18 (2019), 23–48.

⁴³ See H. Murphy and A. Kellow, ‘Forum Shopping in Global Governance: Understanding States, Business and NGOs in Multiple Arenas’, *Global Policy* 4 (2013), 139–149.

⁴⁴ For instance, the Internet Governance Forum (IGF), see www.intgovforum.org/multilingual/; the NetMundial initiative, see <https://netmundial.org/>; and RightsCon, see www.rightscon.org/.

⁴⁵ M. Burri and T. Cottier, ‘Introduction’, in M. Burri and T. Cottier (eds), *Trade Governance in the Digital Age* (Cambridge: Cambridge University Press), 1–14, at 6. See also Chapter 1 in this volume.

The United States has been the key force behind efforts to proliferate its digital trade agenda through international trade law, albeit with a mixed record.⁴⁶ On the one hand, a new generation of mega-regional trade agreements that were negotiated between the United States and like-minded countries incorporate a new set of digital trade rules that introduce horizontal provisions on the free flow of data, such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)⁴⁷ and the United States–Mexico–Canada Agreement (USMCA).⁴⁸ On the other hand, the liberalization of the cross-border flow of data has been controversial in negotiations for the EU–US Transatlantic Trade and Investment Partnership (TTIP) and for a multilateral Trade in Services Agreement (TiSA), which both stalled in 2017 over uncertainties over the stance of the incoming US administration under President Trump.

Repeated efforts to multilateralize digital trade rules through the WTO have not so far yielded tangible outcomes.⁴⁹ Initiated in 1998, the WTO Work Programme on Electronic Commerce has stalled until in early 2019 seventy-six WTO members agreed to launch negotiations on trade-related aspects of electronic commerce.⁵⁰ The resurrection of the e-commerce negotiations, however, takes place during a rather dire crisis of the multilateral forum of the WTO that has left its Appellate Body as a part of the dispute settlement system incapacitated.⁵¹ The very capacity to adjudicate disputes, however, has oftentimes been referred to as the ‘jewel in the crown’ of the WTO that made it the centre of the rule-based international trading system. The timing of the negotiations seems to support Jane Kelsey’s argument that e-commerce has turned into a ‘proxy battleground for the future of the WTO’.⁵²

Absent a broad international consensus in key areas of public interest regulation, already the General Agreement on Trade in Services (GATS)⁵³ curtails a member’s

⁴⁶ See Chapter 2 in this volume.

⁴⁷ The Comprehensive and Progressive Agreement for Transpacific Partnership, available at <http://international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cptpp-ptppg/text-texte/index.aspx?lang=eng>. The CPTPP incorporates by reference the original Trans-Pacific Partnership Agreement (TPP) signed in 2016 and later abandoned by the incoming US administration.

⁴⁸ See Chapter 1 in this volume.

⁴⁹ For an overview of the WTO work on e-commerce, see, e.g., S. Yakovleva and K. Irion, ‘Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade’, *International Data Privacy Law* 10 (2020), 1–21; J. Kelsey, ‘How a TPP-Style E-Commerce Outcome in the WTO Would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO)’, *Journal of International Economic Law* 21 (2018), 273–295; S. Wunsch-Vincent, ‘Trade Rules for the Digital Age’, in M. Panizzon, N. Pohl, and P. Sauvé (eds), *GATS and the Regulation of International Trade in Services* (Cambridge: Cambridge University Press, 2008), 497–529.

⁵⁰ WTO, Joint Statement on Electronic Commerce, WT/L/1056, 25 January 2019.

⁵¹ C. D. Creamer, ‘From the WTO’s Crown Jewel to Its Crown of Thorns’, *AJIL Unbound* 113 (2019), 51–55.

⁵² Kelsey, note 49, at 275.

⁵³ General Agreement on Trade in Services, 15 April 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183 [hereinafter: GATS].

regulatory autonomy by subjecting public interest regulation to certain trade-conforming conditions.⁵⁴ The GATS preamble explicitly recognizes the right of a member state to regulate in order to pursue its national policy objectives.⁵⁵ This right to regulate is however confined as follows: a member may adopt a measure that is from the outset not inconsistent with its GATS commitments or, in case of a GATS inconsistent measure, to justify the measure under one of the general exceptions.⁵⁶ Even though the deregulation of services is not the objective of the GATS,⁵⁷ a member's behind-the-border regulations that aim to afford a high level of protection of human rights run the risk to be deemed protectionist under international trade rules. The EU's regulatory framework on personal data protection makes for a well-researched example. We have concluded elsewhere that 'unreservedly committing to free cross-border data flows likely collides with [the EU's] approach of affording a high level of protection of personal data as is called for by Article 8 of the Charter and as implemented by the GDPR'.⁵⁸

With eminent cross-border trade in AI, individual and societal implications can be critically larger and more pervasive.⁵⁹ The circulation of AI raises the stakes for human rights-based governance given that the technology can be deployed fairly location-independent.⁶⁰ Not only data and machine learning code can be moved across today's digital ecosystem but the predictive outcomes of an AI system can be applied at a distance.⁶¹ Societies have diverse set-ups of rights, freedoms and indeed also ethics. Take facial recognition systems, for example, which are the state policy in China but have prompted calls for strict regulation in Western democracies.⁶² Chander rightly notes in this volume that transnational transplants of AI might prove problematic if they do not correspond to the social and legal contexts of the society it interacts with.

⁵⁴ See, e.g., M. Krajewski, *National Regulation and Trade Liberalization in Services: The Legal Impact of the General Agreement on Trade in Services (GATS) on National Regulatory Autonomy* (The Hague: Kluwer Law International, 2003).

⁵⁵ Recital 3, Preamble to the GATS.

⁵⁶ WTO Appellate Body Report, *Argentina – Measures Relating to Trade in Goods and Services*, WT/DS453/R, adopted 9 May 2016, at para. 6.115.

⁵⁷ P. van den Bossche and W. Zdouc, *The Law and Policy of the World Trade Organization*, 3rd edn (Cambridge: Cambridge University Press, 2014), at 515.

⁵⁸ Yakovleva and Irion, note 49, at 20; K. Irion and S. Yakovleva, 'The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection', *European Data Protection Law Review* 2 (2016), 191–208; S. Yakovleva and K. Irion, 'Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation', *AJIL Unbound* 114 (2020), 10–14.

⁵⁹ See, e.g., M. Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, 2018, available at <https://maliciousaireport.com/>.

⁶⁰ See Chapter 5 in this volume.

⁶¹ K. Irion and J. Williams, *Prospective Policy Study on Artificial Intelligence and EU Trade Policy* (Amsterdam: Institute for Information Law, 2020).

⁶² L. Stark, 'Facial Recognition Is the Plutonium of AI', *XRDS: Crossroads, the ACM Magazine for Students* 25 (2019), 50–55.

The prospect that the first binding framework for the international governance of AI might be international trade law can be frightening unless WTO members retain sufficient margin for experimentation with novel strategies to give effect to human rights in the cross-border context. Susan Aaronson points at the disconnection between efforts to promote the free flow of data and efforts to promote digital human rights at national and international levels.⁶³ As trade agreements have gone beyond import tariffs and quotas into regulatory rules and harmonization, Kelsey has criticized that new e-commerce rules impose ‘significant constraints on the regulatory authority of governments, irrespective of their levels of development, and includes matters that belong more to Internet governance, than to trade’.⁶⁴

E CONCLUSION

Everything is in flux. Cross-border data flows are pervasive and a defining characteristic of the age of digital interdependence. So far, our global information civilization is not founded on a shared commitment to protect human rights regardless of jurisdiction, citizenship and location of data. Engendering respect for human rights remains for the foreseeable future a paramount function of domestic legal institutions which must be reactive to respond to the challenges of cross-border data flows.⁶⁵ We are also beginning to grasp that the challenges for the multi-level governance of human rights are not just about overlapping claims of authority and the transnational export of rules but go to the core of the conditions of human freedom and the democratic constitution of societies.⁶⁶

International trade law is laying claim to the governance of cross-border digital trade and the liberalization of cross-border flow of data. From the domestic protection of data privacy and how data privacy rules may conflict with international trade law, we can draw lessons for the emerging multi-level governance of AI. With respect to AI governance, the EU’s fundamental rights approach holds unique value in an international context where the other major players, like the United States and China, move ahead without paying much attention to these underlying human values. It will be important to critically assess the impact of the WTO e-commerce negotiations on the human rights-based governance of AI before the ‘free trade

⁶³ S. A. Aaronson, ‘Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security’, *World Trade Review* 14 (2015), 671–700.

⁶⁴ Kelsey, note 49, at 256.

⁶⁵ Cohen, note 2, at 238.

⁶⁶ See, e.g., Reidenberg, note 34; H. Farrell and A. L. Newman, *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security* (Princeton, NJ: Princeton University Press, 2019), at 27 et seq.; P. P. Swire and R. E. Litan, ‘None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive’, *Harvard Journal of Law and Technology* 12 (1999), 683–702.

leviathan⁶⁷ further restricts the policy choices not only of individual states but also of the EU itself.⁶⁸

Where international trade rules prevail, they should provide for constitutional pluralism and a sufficient margin for domestic experimentation with novel strategies to give effect to human rights in the online context.⁶⁹ This should not be construed as an argument in favour of a uniform interpretation or even a mandate for the positive harmonization of (digital) human rights through international (trade) law.⁷⁰ Yet, trade law should not move ahead in setting the rules for cross-border trade in the era of big data and AI without recognizing the members' responsibility to take appropriate measures that would ensure that artificial intelligence and overall data governance are fully accountable to domestic human rights frameworks. Identifying strategies and approaches that effectively ground individual interests and societal values in transnational algorithmic systems ought to strike a balance between the rule of law and innovation policy that crucially undergird a robust information civilization.

⁶⁷ G. de Búrca and J. Scott, 'The Impact of the WTO on EU Decision-Making', in G. de Búrca and J. Scott (eds), *The EU and the WTO Legal and Constitutional Issues* (Oxford: Hart Publishing, 2001).

⁶⁸ Irion and Williams, note 61.

⁶⁹ Petersmann, note 6, at 663.

⁷⁰ P. Alston, 'Resisting the Merger and Acquisition of Human Rights by Trade Law: A Reply to Petersmann', *European Journal of International Law* 13 (2002), 815–844.