CHAPTER 9

What kinds of rules are needed to support digital trade?[1]

Martina F. Ferracane and LI Mosi

European University Institute; Shanghai University of International Business and Economics

The prevailing multilateral rules regulating digital trade predate the global internet. Updating them is important, given the trend for countries to embed rules for cross-border trade in digital goods and services in discriminatory free trade agreements. Ongoing negotiations on e-commerce in the World Trade Organization (WTO) on a plurilateral basis offer an opportunity to build on recent regional agreements to agree on rules to support digital trade. Commonalities in the preferences of China and the European Union (EU) on some elements of digital trade policy create prospects for cooperation in this area, thereby helping to keep the WTO relevant in the 21st century.

1. INTRODUCTION

Digital trade is becoming an increasingly important component of global trade, with the Covid-19 pandemic accelerating the pace of digitalisation.[2] The prevailing multilateral rules regulating digital trade predate the global internet as we know it (López González and Ferencz 2018, Ismail 2020), embodied in the WTO's General Agreement on Trade in Services (GATS). Many policymakers, not surprisingly, consider the prevailing rules, negotiated in the early 1990s, to be outdated for the digital era (Wu 2017). An illustration of this is that the classification of services used in the GATS dates to 1991 and is obsolete for the digital era, generating uncertainty whether digital services not included in the GATS list are covered by the commitments undertaken by members. This uncertainty has partially been addressed through dispute settlement, which established that the GATS is technologically neutral. However, there is no explicit language in WTO agreements on data flows, source code, location of computing facilities, and other topics relevant for digital trade.

This situation has paved the way to a wave of 'next-generation' free trade agreements (FTAs) that include binding commitments on digital trade. Two-thirds of the WTO Membership is a party to one or more FTAs that includes e-commerce related provisions

1 Cite as: Ferracane, M F and M Li (2021), 'What kinds of rules are needed to support digital trade?', in B Hoekman, X Tu, and D Wang (eds), *Rebooting Multilateral Trade Cooperation: Perspectives from China and Europe*, CEPR Press, London.

2 Although there is no generally agreed definition, digital trade can broadly be defined as 'the trade of goods and services using the internet, including the transmission of information and data across borders'. Australian government, Department of Foreign Affairs and Trade website. In this paper, digital trade and e-commerce are used interchangeably.

(Burri and Polanco 2020). These agreements provide different levels of commitments on digital trade, with a variety of rules and formulations resulting in a spaghetti bowl that risks instigating a fragmentation of the rules applied to digital trade. In this setting, multilateral discussions are widely seen as crucial to avoid further fragmentation and to lower costs for all firms, especially Micro, Small and Medium Enterprises (MSMEs), to engage in digital trade.

This chapter starts by presenting the history of multilateral discussions on digital trade, from the adoption of the Declaration on Global Electronic Commerce in 1998, to the recent discussions on a Joint Statement Initiative (JSI) on e-commerce. The EU and China are two of the major players in the JSI discussions. We aim to shed light on the possible outcome of the JSI negotiations by presenting the position of these two key actors, drawing on positions taken in ongoing talks, on EU and Chinese commitments on digital trade in their respective FTAs, and developments in domestic regulation.

2. DIGITAL TRADE DISCUSSIONS AT THE WTO

In 1998, at the second WTO Ministerial Conference, WTO members adopted the Declaration on Global Electronic Commerce. This recognised the need to clarify the relationship between trade rules and emerging online modes for trade, and called for the establishment of a work programme on e-commerce (WTO 1998a). In the same declaration, members also adopted the e-commerce moratorium, a commitment to refrain from imposing customs duties on electronic transmissions. Since then, at every Ministerial Conference, the WTO members have agreed 'to maintain the current practice of not imposing customs duties on electronic transmissions'.[3]

The WTO Work Programme on Electronic Commerce, which was established later in 1998, was tasked with exploring WTO rules and the production, distribution, marketing, sale or delivery of goods and services by electronic means (WTO 1998b). This work programme did not lead to new rules for digital trade. The only adjustments to the rulebook made after the entry into force of the WTO affecting digital trade was the Information Technology Agreement (ITA), and its update in 2015.

The ITA is of particular significance to digital trade. The WTO members committed themselves to reduce their tariffs on IT goods in four steps of 25% to reach a tariff-free policy by the year 2000. This obligation pertains to a common list of IT products covering a wide range of some 180 information technology products in five major categories: computers and peripheral devices, semiconductors, printed circuit boards, telecommunications equipment (except satellites), and software. By the year 2015, the ITA covered 95% of the existing world trade in IT goods (WTO 2017a). At the Nairobi

3 At the 11th Ministerial Conference in Buenos Aires in 2017, the moratorium was agreed in the final hours of the conference. This was due to debates on the implications of the moratorium on developing countries in terms of loss of tax revenues.

Ministerial Conference in December 2015, over 50 members also concluded the expansion of the ITA, which now covers an additional 201 products valued at over $1.3 trillion per year.[4]

Other than the commitments taken on digital goods under ITA, discussions on digital trade did not see any significant progress until the Nairobi Ministerial Conference in 2015, which signalled willingness by many WTO members to explore new approaches to the negotiations (WTO 2015) and calling for e-commerce to be a priority among 'new issues' for discussion and consideration (Ismail 2020).

In parallel, in the 2010s, the US started to pursue new rules, including the upgrade of the moratorium into a permanent commitment and pushing the WTO to change the mandate of the Work Programme from discussions to negotiations (Azmeh et al. 2020, WTO 2011a, WTO 2011b, WTO 2014). The EU joined these efforts, but with more modest objectives. In 2016, the MIKTA group (Mexico, Indonesia, Korea, Turkey, and Australia) issued a statement arguing that the WTO should focus more attention on the digital trade agenda and that the organisation had an important role to play to keep the digital markets open, create a facilitating environment for digital trade, promote consumer confidence, and support small and medium-sized enterprises (SMEs) to engage in digital trade. The group called for efforts to consider both existing and newer e-commerce issues (MIKTA 2016).

In 2017, a 'Friends of E-commerce for Development' group called for more focus on e-commerce as an engine of development and growth.[5] In particular, the group called for more focus in the WTO and other international organisations on a range of issues, particularly concerning e-commerce readiness and strategy, ICT infrastructure and services, trade logistics, payment solutions, legal and regulatory frameworks, e-commerce skills development and technical assistance, and access to financing (Friends of E-Commerce for Development 2017).

Discussions on e-commerce intensified in the run-up to the 11th Ministerial Conference in Buenos Aires in 2017, which saw the release of a Joint Statement on e-commerce, signed by 71 countries, reaffirming the importance of e-commerce and the goal of advancing e-commerce work in the WTO (WTO 2017b). The group announced the start of exploratory work toward WTO negotiations on trade-related aspects of e-commerce and set the ground for the start of plurilateral negotiations on e-commerce. The argument for starting plurilateral discussions at the WTO is that the high number of WTO members and the complexity of issues make decision-making through the consensus and single undertaking principles highly difficult, which could ultimately weaken the multilateral regime as members enact new rules in bilateral and regional trade agreements.

4 See the WTO webpage on the Information Technology Agreement: https://www.wto.org/english/tratop_e/inftec_e/inftec_e.htm (last accessed in May 2021).

5 This group includes Argentina, Chile, Colombia, Costa Rica, Kenya, Mexico, Nigeria, Pakistan, Sri Lanka, and Uruguay.

This initiative faced strong opposition by some developing countries, including India, South Africa, and the Africa Group in the WTO. The latter argued that 'it is perplexing that some members are advocating for new multilateral rules on e-commerce' and that 'the multilateral rules as they are, are constraining our domestic policy space and ability to industrialise' (WTO 2017c). These countries also expressed fears on a commitment to free flow of data that would provide free market access to digitally delivered goods and services, depriving developing economies of substantial tariff revenues as more goods are digitized, and threats to their domestic services industry as more services are traded online.

In 2019, 76 members signed a second Joint Statement on e-commerce, and formally announced in Davos the willingness to begin the plurilateral negotiation process to advance discussions. Throughout 2019, the group held negotiations, albeit in different settings. Despite the challenges presented by Covid-19, the number of participants in the initiative has grown to 86 WTO members, collectively accounting for over 90% of global trade and representing all major geographical regions and levels of development (WTO 2020). However, participation by least developed countries (LDCs) and members from Africa, Caribbean, and Pacific regions has remained limited. Reasons highlighted for the limited participation include fears of weakening multilateralism and limited benefits for low-income countries (WTO 2019a).

A draft consolidated text was circulated among participants on 7 December 2020. The text is based on members' proposals that cover the following themes: enabling e-commerce, openness and e-commerce, trust and e-commerce, cross-cutting issues, telecommunications, market access, and scope and general provisions. The negotiation process is being led mainly by Australia, Japan, and Singapore, who are aiming for significant advances in negotiations by the advent of the 12th Ministerial Conference (MC12). The negotiations are not expected to be finalised during MC12, which was postponed to November 2021 as a result of the Covid-19 pandemic. As of yet, there is no agreement on several key issues, and uncertainty also remains concerning the legal form through which any outcome will be integrated in the WTO.

One of the main issues blocking progress on digital trade on the WTO agenda is the question of categorisation. WTO members differ in opinion on whether products which were usually sold as goods due to their link to a physical carrier, and which can now be delivered online (e.g. music or movies), shall be treated as goods under the General Agreement on Tariffs and Trade (GATT) or as services under GATS (Bergemann 2002). If goods delivered online were to be considered goods, they would be subject to trade restrictions such as tariffs (Baker et al. 2001). On the other hand, if goods delivered online were to be considered services, they would be subject to market access barriers and discriminatory domestic regulations. Until the classification debate is resolved, WTO members decided not to impose tariffs on imported electronic transmissions. Other issues

which remain highly controversial include the classification of digital services, restrictions on the transfers of data, requirements for local data processing, and computing facilities and transfers of source code.

3. DIGITAL TRADE IN FTAS SIGNED BY THE EU AND CHINA

Given the lack of progress made in the work programme discussions launched in 1998 on e-commerce, negotiations shifted to bilateral and regional fora.[6] As a result, the scope and depth of commitments on digital trade in FTAs has expanded to cover a broader range of issues, responding to the enactment of new types of measures imposed by governments (Wu 2017).

3.1 Digital trade in EU FTAs

The EU has actively sought to include e-commerce chapters in their FTAs. The first EU trade agreement to include an e-commerce chapter was the EU-CARIFORUM Economic Partnership Agreement (EPA), which entered into force in 2008.[7] While other advanced economies have usually sought to include broad-reaching e-commerce chapters in their agreements, the EU represents an exception. The e-commerce sections of the EU's trade agreements tend to focus primarily on information exchange and the promotion of regulatory dialogue, rather than more robust substantive provisions that cater for digital trade (Wu 2017, Micallef 2019). EU agreements usually include an obligation to not impose customs duties on digital products, facilitating commerce in downloadable products such as software, e-books, music, movies, and other digital media. These types of provisions are common among agreements covering e-commerce. In some cases, this represents the only binding commitments on e-commerce in EU agreements, as in the case of the EU-Central America Association Agreement, which additionally contains a provision on establishing a regulatory dialogue (Article 201).

EU trade agreements also include provisions that extend national treatment and MFN disciplines to the digital realm. More recent FTAs also include the principle of technological neutrality to clarify the scope of the commitments to include digital services. This provision first appeared in the EU-Singapore FTA (Article 8.59), noting that measures related to the supply of services using electronic means fall within the scope of the obligations contained in the relevant provisions in the chapter on services, establishment, and e-commerce as a whole.

6 The first FTA to include an explicit standalone chapter to address e-commerce was the one between Australia and Singapore, which entered into force in July 2003. Other agreements in the early 2000s which included e-commerce articles or sections are US-Chile FTA, US-Singapore FTA, US-Australia FTA, and Thailand-Australia FTA.

7 The EC-Chile from 2003 included a limited article covering basic cooperation in e-commerce, but did not have a dedicated chapter.

Provisions on digital authentication and/or e-signatures are also very common in FTAs with an e-commerce chapter. Commitments taken by the EU in this area appear lighter-touch compared to non-EU FTAs. Rather than requiring firm commitments, EU trade agreements seek to establish a dialogue on regulatory issues that includes 'the recognition of certifications of electronic signatures issued by the public and the facilitation of cross-border certification services' (Wu 2017).[8] The EU-Singapore FTA contains a dedicated article (Article 8.60), in which the parties commit to 'take steps to facilitate the better understanding of each other's electronic signatures framework (...) and to examine the feasibility of having in the future a mutual recognition agreement on electronic signatures'.

Provisions on paperless trade are not included in most EU FTAs, the exception being EU-Colombia and EU-Peru (Article 165) and EU-Korea FTA (Article 7.49). These provisions seek to make the process of making trade administration documentation available in digital format and of allowing importers and exporters to submit documentation electronically. Regarding consumer protection online, the primary emphasis of EU FTAs is on regulatory dialogue,[9] in contrast to non-EU FTAs that have opted for binding commitments on consumer protection online, aiming at curtailing potential harm from online purchases and increasing the trust of consumers in doing business electronically.

The topic of unsolicited electronic messages (spam) is frequently found in EU trade agreements. The provision is consistent across the agreements, and it is limited to maintaining a regulatory dialogue on policies towards unsolicited electronic commercial communications.[10] EU agreements commonly call out important policy areas in which cooperation is relevant and place major emphasis on regulatory dialogue. In some cases, there are provisions directly addressing the delivery of technical assistance and capacity building from the EU to its trading partner.[11]

A key digital trade policy issue is the treatment of data flows. Starting from 2018, when for the first time a ban on cross-border restrictions was agreed in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), several 'next generation' agreements have included binding commitments on data flows. This is not the case for the EU, where this issue has been controversial (Yakovlela and Irion 2020). Although the EU agreed to specific commitments on cross-border data flows related to financial services, e.g. in the EU-Korea FTA in 2011,[12] strong voices have opposed the inclusion of horizontal binding commitments on free data flows in EU FTAs. Concerns relate to the protection of privacy, as well as market power of US digital firms.[13] An illustration of this, is a report

8 See e.g. EU-Korea FTA (Article 7.49.1), EU-Moldova FTA (Article 255.1).
9 See e.g. EU-Central America Association Agreement (Article 202), EU-Georgia Association Agreement (Article. 128).
10 See e.g. EU-Korea FTA (article 7.49), EU-Central America Association Agreement (Article 202).
11 See e.g. EU-CARIFORUM Economic Partnership Agreement, Article. 121.
12 Under Annex 13-B, the parties agreed to 'allow a financial institution of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the institution's ordinary course of business'.
13 While the EU as a whole is generally supportive of the inclusion of binding commitments to free cross-border data flows, France and Germany expressed some concerns (Azmeh et al. 2020). Such lack of support reflected both economic and technological concerns by those countries on the impact of such clauses on the European economy in the context of dominance of large US digital firms and also concerns about implications of such rules on privacy and data protection.

by the French Digital Council, an independent advisory commission on digital issues established by the French President, issued on the negotiation of digital issues in TTIP recommending that Europe should 'play for time in the negotiations, step up construction of Europe's digital strategy, and strengthen the European Union's bargaining capacity' (CNNum 2017, at 13, as cited by Azmeh et al. 2020). Conversely, other member states have been calling on the European Commission to address cross-border data flows in trade agreements in an ambitious manner.[14]

The initial position of the EU, as reflected in the EU-Japan Economic Partnership Agreement (EPA) and in the negotiations for a FTA with Mexico, was to insert a placeholder on cross-border data flows to enable the parties to revisit the issue in three years. In parallel, internal EU debates resulted in the adoption of horizontal provisions for cross-border data flows and for personal data protection. These provisions, which are designed to be inserted in all EU future FTAs, consist of three articles:[15]

- The first commits the parties to 'ensuring cross-border data flows to facilitate trade in the digital economy' and outlines four mechanism parties commit not to use: (i) requiring the use of computing facilities or network elements in the party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a party; (ii) requiring the localisation of data in the party's territory for storage or processing; (iii) prohibiting storage or processing in the territory of the other party; (iv) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the parties' territory or upon localisation requirements in the parties' territory. Article A also includes a mechanism to review the implementation of this provision three years after the entry into force of the agreement.
- The second commits parties to recognise that the protection of personal data and privacy is a fundamental right and that 'high standards in this regard contribute to trust in the digital economy and to the development of trade'. Personal data is defined in the agreement to mean 'any information relating to an identified or identifiable natural person'. The article allows each party to adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy 'including through the adoption and application of rules for the cross-border transfer of personal data' and stresses that 'nothing in this agreement shall affect the protection of personal data and privacy afforded by the parties' respective safeguards'.

14 See for example the letter on data flows to the Vice President of the European Commission, Frans Timmermans, dated 16 May 2017, available at: https://www.government.nl/documents/letters/2017/05/19/like-minded-letter-on-data-flows-in-trade-agreements.

15 This text has been tabled for the first time in the trade agreement's negotiations with Indonesia.

- The third article commits parties to 'maintain a dialogue on regulatory issues raised by digital trade', including the recognition and facilitation of interoperable cross-border electronic trust and authentication services, the treatment of direct marketing communications, the protection of consumers in the ambit of e-commerce, and any other issue relevant for the development of digital trade. The focus of such cooperation will be on exchanging information on the parties' respective legislation on these issues as well as on the implementation of such legislation. Importantly, this article explicitly excludes provisions related to protection of personal data and privacy including on cross-border data transfers of personal data from such dialogue, which follow a different process.[16]

Commenting on the decision to grant data adequacy status to Japan, the European Commission stressed that 'For the EU, privacy is not a commodity to be traded. Dialogues on data protection and trade negotiations with third countries have to follow separate tracks' (European Commission 2018). Through this mechanism, the EU aims to move toward free flow of data with its trading partners while maintaining its relatively strong measures in the area of privacy and personal data protection.

Despite the prominent domestic debate on the protection of personal information, European negotiators have not proactively sought to include an obligation on this issue in FTAs until recently. Instead, APEC[17] members have taken the lead in pushing for inclusion of such provisions in FTAs (Wu 2017). Some EU agreements use weak or hortatory language on data protection in the trade agreement with Colombia and Peru, which states that the partiers 'shall endeavour, insofar as possible, and within their respective competencies' to develop or maintain regulations for the protection of personal data (Article 164).

Another issue which is virtually absent from EU FTAs is the requirement for the government to limit the requests of disclosure of source code as a condition for doing business in the country. This requirement is only present in the agreement with Japan (Article 8.73) and with the UK (Article DIGIT.12).[18]

All in all, the EU's approach to digital trade has emphasised regulatory dialogue and does not address a range of issues which can be found in FTAs implemented by other advanced economies such as Australia, Japan, and the US. This has begun to change recently with the EU-Japan EPA building upon in the modernised EU-Mexico Trade Agreement,[19] and the EU-UK Trade and Cooperation Agreement. The EU-Japan EPA addresses for the first

16 The GDPR adequacy decision is adopted through a proposal by the European Commission followed by an opinion of the European Data Protection Board, an approval from representatives of EU countries, and a final adoption by the Commission.

17 Asia-Pacific Economic Cooperation.

18 The Trade and Cooperation Agreement is provisionally applicable from 1 January 2021, after having been agreed by EU and UK negotiators on 24 December 2020.

19 The text has been agreed, but the agreement has not yet entered into force: https://ec.europa.eu/trade/policy/in-focus/eu-mexico-trade-agreement/.

time issues such as data transfer and access to source code, including endeavours not to impose prior authorisation on the provision of services by electronic means (Article 8.75), the conclusion of contracts by electronic means (Article 8.76), a binding commitment on electronic signatures (Article 8.77), binding obligations on spam (Article 8.79). Given the fact that the EU is discussing similar language in on-going negotiations, the EU-Japan agreement is expected to serve as a basis for the EU in negotiations under the JSI.[20]

3.2 Digital trade in China's FTAs

Before the Regional Comprehensive Economic Partnership (RCEP), China had signed only four FTAs which included e-commerce provisions. These are the China-Korea FTA (2015), the China-Australia FTA (2015), and the China-Singapore FTA Upgrade (2018) and China-Cambodia FTA (2020). The e-commerce provisions in the above-mentioned agreements are mostly shallow rules, dealing with matters such as electronic authentication and electronic signature, online consumer protection, personal information protection, and paperless trading. The provisions are relatively simple, some are only stipulated in principle, and some are not legally binding. The dispute settlement mechanisms do not apply to any dispute arising under the e-commerce chapters in these FTAs.

To date, the RCEP is the highest standard FTA that China has signed. Chapter 12 on e-commerce includes provisions on paperless trading, electronic certification and signature, online consumer protection, online personal information protection, and network security, among other issues. While RCEP membership implies that China has agreed for the first time to provisions on cross-border transfer of information by electronic means and location of computing facilities in an FTA, compared with other recent FTAs such as the CPTPP, RCEP's e-commerce rules are less ambitious. RCEP has no commitments related to source code and permits significant latitude for measures that do not meet the requirements of cross-border free flows of data and prohibition of data localisation.

Both Article 12.14 'Location of Computing Facilities' and Article 12.15 'Cross-Border Transfer of Information by Electronic Means' stipulate that 'nothing in this Article shall prevent a Party from adopting or maintaining any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties'. In addition, both Article 12.14 and Article 12.15 include a footnote stating that 'the Parties affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party'. The necessity of a measure to achieve a legitimate policy objective is therefore considered to be self-judging. If RCEP signatories cannot resolve a dispute through consultation, the matter is to be addressed by the RCEP Joint Committee (ministerial level). However, the Committee does not have the power to impose any decision (Leblond 2020).

20 The modernised EU-Mexico Trade Agreements also adds an important Article on open internet access for users (Article 10).

The RCEP provisions on digital trade demonstrate that China recognises the importance of policies affecting cross-border data flows and has accepted a number of guiding principles for domestic laws and regulations. The RCEP Chapter on e-commerce is a good harbinger of the kind of agreement that can be expected from the JSI negotiations on e-commerce, providing a baseline for what China could accept in terms of digital trade provisions.

4. DOMESTIC REGULATORY TRENDS

Recent developments in domestic regulation affecting digital trade provide further context on how sensitive issues are being addressed in the EU and China. These show how similar issues are being addressed in different ways, potentially raising costs for businesses to conduct digital trade.

4.1 The EU

The political guidelines for the next European Commission 2019-2024, put forward by Ursula von der Leyen, reflect the political ambition of a 'stronger Europe in the world'. The regulation of digital trade has mostly taken place in a defensive manner, although the EU has taken a proactive approach in addressing complex issues such as data protection and competition issues. In recent years, the EU has started to strongly emphasise 'digital sovereignty'. This approach emerges clearly in the recent Communication on 'A European strategy for data', which states that 'free and safe flow of data should be ensured with third countries, subject to exceptions and restrictions for public security, public order, and other legitimate public policy objectives of the European Union'.[21]

The EU's defensive stance reflects several factors, including the dominance of US and Chinese firms in the digital sectors, concerns on the ability to ensure the privacy of EU citizens, and the security risks associated with foreign technologies (EPRS 2020a). The EU internal policy is characterised by a number of emerging initiatives that look to reduce fragmentation of the EU and to create a fair and competitive market for EU firms. This section highlights some of the initiatives which help to understand the EU's stance on digital trade.

4.1.1 GDPR and the Brussels effect

The General Data Protection Regulation (GDPR) is one of the most comprehensive frameworks in the world for the protection of personal data.[22] It builds on the 1995 European Directive on data protection, which already provided extensive regulatory

21 The text continues by arguing that 'this would allow the EU to have an open but assertive international data approach based on its values and strategic interests', European Commission (2020), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions: A European Strategy For Data*, COM(2020) 66, Brussels.

22 Regulation (EU) 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).

safeguards to ensure a high level of protection domestically and cross-border. The main novelties of the GDPR are the extra-territorial approach and high fines. In fact, even if a company does not have a physical presence in the EU, it has to comply with the GDPR if the business activities include offering digital products/services within the EU or monitoring the behaviour of EU residents (Article 3 (2)). The fundamental approach of the GDPR is that personal data can be transferred and processed outside the EU only if there is full compliance with the privacy rights provided to EU citizens. To that effect, personal data transfers are allowed only to specific countries whose regime is considered 'essentially equivalent' to the GDPR or if the data processor can offer appropriate safeguards including binding corporate rules (BCRs) that allows intra-company transfers, standard contractual clauses (SCC) approved for intra-company transfers or with certification mechanisms. Alternatively, the data can be transferred only if some derogations apply, including the explicit consent of the data subject and the necessity of the transfer for the performance of the contract. These derogations can be used only in specific situations and not for day-to-day transfers.

The EU approach has become a *de facto* global standard for many countries when it comes to designing data protection rules. This 'Brussels effect'[23] is reflected in many countries adopting GDPR-like frameworks. This may be in the hope to be accorded adequacy status by the EU in the future, and therefore facilitate the access to the EU market, and/or it may reflect a view that the EU approach constitutes good practice.

4.1.2 The invalidation of the Privacy Shield

While the GDPR recognises the importance of cross-border data flows for trade and international cooperation (Recital 101), the recent decision of the European Court of Justice (ECJ) in *Scherms II* raises some doubts about the future of data flows from the EU.[24] The ECJ decision invalidated the *Privacy Shield*, which was a mechanism put in place to provide adequacy to transfers to selected US companies who followed certain rules. In the dispute, the ECJ found that the data surveillance laws in the United States, in particular Section 701 of the Foreign Intelligence Surveillance Act and Executive Order 12333, were not consistent with the GDPR, and therefore the Privacy Shield mechanism was invalid. It also upheld the validity of the Standard Contract Clauses (SCCs), but it provided that companies using SCCs might need to adopt supplementary measures to ensure adequate protections.[25]

23 See Bradford, A (2020), *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, ISBN: 9780190088583.

24 Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18.

25 For more information, see the EDPB Recommendations 01/2020 on measures that supplement transfers tools to ensure compliance with the EU level of protection of personal data, 11 November 2020.

4.1.3 GAIA X

The recent initiative proposed by France and Germany points to the objective of digital sovereignty in the EU. The project aims to set up 'high performance, competitive, secure and trustworthy data infrastructure for Europe'[26] that achieves 'high aspirations in terms of digital sovereignty while promoting innovations'.[27] In practice, the project aims to enable a federated cloud infrastructure for the European market to facilitate interoperable data exchange in the EU. While foreign companies are not precluded from participating, it is expected that the project will be a tool to boost the EU digital sector and enhance the ability of governments to enforce the adoption of EU data protection standards.[28]

4.1.4 Data Governance Act

The Data Governance Act (DGA) aims to improve the availability of data and to strengthen data sharing in the EU through mechanisms that facilitate the reuse of public sector data. The strategy argues that 'the digital transformation of the EU economy depends on the availability and update of secure, energy-efficient, affordable and secure data processing capacities, such as those offered by cloud infrastructure and services, both in data centres and at the edge' and that the EU 'needs to reduce its technological dependencies in these strategic infrastructures, at the centre of the data economy'.[29] The proposal also contains provisions that restrict the transfer of non-personal data outside the EU. For instance, public data can be transferred outside the EU to countries that provide 'equivalent measures' for protecting intellectual property and trade secrets. In the absence of adequate safeguards, transfers could only be conducted if the entity reusing the data undertakes the obligations to protect the data consistent with EU standards and accepts the jurisdiction of the courts of the EU member states regarding any dispute related to compliance. The proposal also recognises that stricter standards may be necessary for transfer of highly sensitive non-personal data such as health data.

26 German Federal Ministry for Economic Affairs and Energy (2019), Project GAIA-X: A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem, Executive Summary, 29 October 2019, available at https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/das-projekt-gaia-x-executive-summary.pdf.

27 See Gaia-X website: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html (last accessed in May 2021).

28 European Council Conclusions, Special meeting of the European Council (1 and 2 October 2020), EUCO 13/20, at point 7, Brussels, 2 October 2020.

29 Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), COM/2020/767 final, 25 November 2020, Brussels.

Other recent proposals[30]

The EU has also pushed forward several additional proposals, which are likely to have an impact on the e-commerce negotiations, as they include issues such as the access to source code by government authorities and intermediary liability. The most relevant proposals are the Digital Services Act,[31] the Digital Markets Act,[32] and the Artificial Intelligence Act.[33]

4.2 China

The Cyberspace Administration of China is the main regulatory authority for data flows coordinating China's cyber policy. In addition, China has sectoral regulations for certain types of data flows. For example, the People's Bank of China is responsible for regulating financial data and the National Health Commission is responsible for regulating personal health information.

China has moved rapidly to construct a policy and regulatory framework on data flows. The framework covers different policies, laws, and regulations, as well as national standards. In 2016, the State Council launched *Several Opinions on Promoting Information Development and Effectively Protecting Information Security*, requiring that data centres and cloud computing platforms which provide services for the government should be established within China.

In addition, there are several laws and regulations adopted in the past five years. The *Cybersecurity Law* is at the centre. Its implementation rules, such as *Draft Measures on Security Assessment for Personal Information Cross-Border Transfer* and *Draft Regulations on Protecting the Security of Key Information Infrastructure* are still in draft form. In 2020, China adopted the *Data Security Law* and released the *Draft Personal Information Protection Law*. These two laws, together with the Cybersecurity Law, will comprise the three pillars for data governance regime in China.

The national standards on data transfer are not legally binding. But regulatory authorities frequently rely on these standards to implement laws and regulations. As the corresponding standard of the *Cybersecurity Law*, the *Draft Guidelines for Cross-Border Data Transfer Security Assessment* (hereinafter referred to as *Draft Security Assessment Guidelines*) provide the relevant processes and standards that will apply when conducting security assessments before transferring personal information outside of China.

30 For a summary of recent proposals, see also Congressional Research Services (2021), *EU Digital Policy and International Trade*, R46732, 25 March 2021.

31 Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final.

32 Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final.

33 Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final.

The *Cybersecurity Law* and its implementation rules not only cover personal information, but also so-called 'important data'. According to the *Draft Security Assessment Guidelines*, 'important data' means data that is very closely related to China's national security, economic development, or societal public interests. Pursuant to Annex A of the guidelines, important data tends to be relevant in several industries, including energy, environment, manufacturing, and military.

The *Data Security Law* shall apply to all data activities carried out within China. It will also establish extraterritorial jurisdiction over foreign entities that engage in data activities inside and outside of China, that harm national security or public interest. Since security is a consistent theme of the law, it has established a national security review system to review any data activities that affect, or may affect, national security. The law also implements export control on data that are controlled items related to the fulfilment of international obligations and national security. To identify what kind of data that are controlled items need to refer to the *Export Control Law*, which was also adopted in 2020

Releasing the *Draft Personal Information Protection Law* is a high-profile move, since there is no overarching personal data protection law in China yet. The draft law includes some provisions on cross-border data transfer, including security assessment requirements under specified circumstances, which is aligned with the *Cybersecurity Law*. The draft law also provides for extra-territorial application. It shall apply not only to the processing of personal information within China, but also to cross-border processing activities of personal information of Chinese citizens. Overseas processors are required to establish a specialised agency or appoint a representative within China.

There are several sector specific laws and regulations covering data flows, including financial data, personal health data, online services data, and others. As for financial data, the regulations provide that the credit information and personal financial data shall be stored, processed, and analysed within China. Similar requirements apply to personal health information. Online services data covers online publishing, internet maps, online taxi booking, etc. The main policy rationales for these requirements appear to be cybersecurity, personal information protection, data security, and government access to data. However, it is likely that the main concerns of the Chinese government are internet governance capability, domestic regulatory framework, and jurisdiction.

Firstly, the internet governance capabilities need to be strengthened. Although China is seeking to build a comprehensive cyber governance system, it is far from effective and strong enough. China's cyber governance has arguably received the fiercest criticism for maintaining government control of cyberspace. But in fact, it is about the regulatory capability of addressing substantial cybersecurity challenges, such as cyber attacks, cyber scams, and personal data breaches. Just take data breaches, for example, where internet

users suffer the most serious data breaches. According to a report by China Consumers Association, over 90% of mobile apps collect too much data, and more than 85% of China's app users have had their data leaked.[34]

Secondly, the domestic legal system needs to be improved. Several relevant and important laws remain under development, which leaves legal uncertainties for data flows. There is no overarching personal data protection law in China yet. In 2020, China released the *Draft Law on Personal Information Protection*, which requires conducting security assessments when critical information infrastructure operators transfer personal information across the border. China has also released the *Draft Law on Data Security Law*, stipulating that China will promote the safe and free flow of data across borders.

Thirdly, there are difficulties in exercising jurisdiction. The key issue is how to exercise jurisdiction if there is no local presence. In theory, companies doing business in a country have a legal 'nexus' with that country, which puts the company in that country's jurisdiction. But when it comes to online cross-border supply, the nexus is not strong enough. Law enforcement authorities are unable to easily enforce their decisions, because those decisions require cooperation from relevant actors from other jurisdictions. Mutual legal assistance and law enforcement cooperation is often time-consuming and unpredictable. Extraterritorial jurisdiction, like the *US Clarifying Lawful Overseas Use of Data Act*, will inevitably lead to a conflict of jurisdiction with the country where the data is located.

5. POSITIONS IN THE WTO E-COMMERCE NEGOTIATIONS

5.1 EU

In April 2019, the EU released its proposal on WTO disciplines and commitments related to e-commerce and telecommunication services under the JSI. The proposal is ambitious in ensuring functional data flows for businesses, improving market access and regulatory predictability, while remaining committed to consumer protection and data protection, and includes the following elements (EPRS 2020b):

1. In terms of enabling e-commerce, in particular for SMEs, the EU proposes common rules for improving the recognition of e-contracts and e-signatures.
2. The principle of open internet access, subject to applicable rules, as well as reasonable and non-discriminatory network management. The EU proposal seeks to balance the free flow of data for business purposes with a commitment to personal privacy, which it considers a fundamental right. Enterprises should

34 https://www.sixthtone.com/news/1003278/90-percent-of-chinese-apps-surveyed-over-collect-data-

not be restricted by requirements to localise data or computer facilities in a given member's territory. At the same time, members need to be free to adopt rules that protect personal data and privacy, as they deem necessary.

3. To build trust in e-commerce, the EU proposes to improve consumer protection by requiring measures against unsolicited emails (spam). The EU suggests that members also put in place measures against fraudulent and deceptive practices, and potentially measures that require traders to act in good faith, provide accurate information, and grant consumers access to redress.
4. On cross-cutting issues, the EU proposes to improve transparency and regulatory predictability.
5. With regard to telecommunications, the EU proposes to revise rules for telecommunications services, such as tackling anti-competitive practices and enabling interconnectivity between suppliers, and to improve market access for computer services.
6. A prohibition on governments requiring the transfer of, or access to, source code (human-readable programmes), except in special cases such as the enforcement of intellectual property rights or for competition law purposes.
7. A commitment to refrain permanently from imposing customs duties on electronic transmissions (e.g. movies, emails, software).
8. Greater participation by WTO members in the ITA and its product coverage expansion.
9. Exclusion of cultural and audio-visual issues from the scope of the negotiations to protect cultural diversity.

The Trade Policy Review communication published in February 2021 by the European Commission makes clear that digital trade is a priority for EU trade policy, and that the EU intends to play a central role in shaping the global rules under the WTO.[35]

5.2 China

China has elaborated its position regarding the WTO e-commerce negotiations in its communications to the WTO. China stressed that 'the negotiation should set a reasonable level of ambition with full consideration of members' right to regulate, strike a balance among technological advancement, business development, and legitimate public policy

35 European Commission (2021), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Trade Policy Review - An Open, Sustainable and Assertive Trade Policy, COM(2021) 66 final.

objectives of members, such as internet sovereignty, data security, privacy protection, etc., and reach a balanced, pragmatic outcome reflecting all members' interests through equal consultation' (WTO 2019b).

China's proposal focuses on the discussion of cross-border trade in goods enabled by the internet, together with relevant payment and logistics services, while paying attention to the digitalisation trend of trade in services, and exploring the way to develop international rules for e-commerce centring on a sound transaction environment and a safe and trustworthy market environment.

There are four action areas in China's position in the WTO negotiations under the JSI:

1. Clarify the definition of trade-related aspects of e-commerce and future rules' scope of application, including the trade-related aspects of e-commerce, electronic transmission, etc.
2. Establish a sound environment for e-commerce transaction, including facilitating cross-border e-commerce, paperless trading, electronic signatures and electronic authentication, electronic contracts, moratorium of customs duties on electronic transmissions.
3. Create a safe and trust-worthy market environment for e-commerce, including online consumer protection, personal information protection, unsolicited electronic commercial messages, cyber security, and transparency.
4. Promote pragmatic and inclusive development cooperation, including to bridge the digital divide, support research, training and communication and e-commerce for development programmes.

China has noted that issues such as cyber security, data safety, and privacy are increasingly highlighted, bringing unprecedented security risks and regulatory challenges to members. China has argued that associated issues such as data flow, data storage, and treatment of digital products need more exploratory discussions before being incorporated into WTO negotiations, to allow members to fully understand their implications and impacts, as well as the related challenges and opportunities.

6. CONCLUSIONS

The prevailing multilateral rules regulating digital trade predate the global internet. Updating them is important, given the trend for countries to embed rules for cross-border trade in digital goods and services in discriminatory free trade agreements. The launch of WTO e-commerce JSI negotiations on a plurilateral basis should be seen as major progress in WTO e-commerce discussions, which reflects the new demands for international trade rules on e-commerce. These ongoing negotiations offer an opportunity to build on recent regional agreements to agree on rules to support digital trade.

While the EU and China have different starting points on the WTO e-commerce negotiations, the respective approaches seem to point towards scope for convergence on several topics. These commonalities in the preferences on some elements of digital trade policy create prospects for cooperation in this area. Yet, whether the two major trade powers can help address obvious differences among the parties in the JSI negotiations remains to be seen. Some topics remain contentious, such as permanent moratorium of customs duties on electronic transmissions, non-discrimination treatment of digital products, cross-border free data flow, and transfer of source code. The divergences not only reflect the conflicts between trade liberalisation and non-trade goals, but also the interrelationship between digital trade policies and broader internet governance challenges.

While the JSI can play an important role in confirming key principles and good practices, which have been embodied in 'next-generation' FTAs, such as CPTPP, Digital Economy Partnership Agreements, and the ASEAN e-commerce agreement, an ambitious agreement covering issues such as data flows and source code seems unlikely given the large number of countries involved in the JSI discussions and the diverging positions of China, the EU, and the US on key subjects. Reconciling the positions of the major players in the negotiations is essential to the success of the e-commerce talks.

Even if some issues cannot be resolved, the JSI negotiations can improve the governance of digital trade by promoting transparency, enhancing predictability, and establishing a mechanism for regulatory cooperation on interoperability and, eventually, greater harmonisation of regulatory regimes. To this end, the following points might be considered:

1. The agreement should promote transparency. This can be done through the publication of current measures and proposals relating to e-commerce and by offering the opportunity to members to comments on those measures.

2. In order to reduce ambiguity, the negotiators should clarify the definition and scope of e-commerce and shed light on whether the rules will take the form of a self-standing agreement (and if so, its relationship with existing WTO agreements) or will instead entail a modification of existing provisions. The accession mechanism should be clarified, and it should be ensured that the market access and national treatment commitments are compatible with GATS. A positive list approach might support the multilateralisation of the agreement, while a negative list would require further thought on how to make the system compatible with current commitments. Several developing countries have pointed out that a negative list approach can bring them considerable challenges, and that the establishment of a separate agreement would create uncertainty on how the GATT, the GATS, and other related agreements apply to e-commerce.

3. To support the inclusion of LDCs, the negotiations could establish an open plurilateral agreement, which, in contrast with an exclusive agreement, is implemented on the basis of most-favoured-nation (MFN) treatment. An open agreement would enable all countries outside the current negotiations, which are mostly developing and least-developed countries, to enjoy the benefits of the agreement, while not having to assume corresponding obligations. This would help them integrate into global e-commerce and global value chains and would be in line with the objective of the WTO e-commerce negotiations to 'further enhance the benefits of e-commerce for businesses, consumers and the global economy' (WTO 2019a).

4. Regulatory cooperation, whether in form of structured dialogue or ad hoc conversations, should be encouraged to allow members to address the cross-border nature of e-commerce, and can contribute to the exchange of good practices. Cooperation is the starting point for clarifying different regulatory regimes with the view of promoting harmonisation.

5. Efforts for harmonising and consolidating digital trade rules can be crucial to reap the benefits of digitalisation in the coming years. As already stipulated in the Agreement on Technical Barriers to Trade (TBT), relevant international standards such as International Organization for Standardization (ISO) and Institute of Electrical and Electronics Engineers (IEEE) can be the basis for creating digital trade rules. Therefore, collaboration in standard setting activities can be an important component in the overall architecture of the JSI. Involvement of business and international organisation should also be considered, given that certain issues can be very technical in nature.

6. Where harmonisation is not practical or politically feasible, finding bridging mechanisms between different regimes may be useful to find common ground. Promoting interoperability between the approaches brought forward by heterogeneous members would be a good first step.

7. For sensitive issues on which negotiators cannot agree, soft law provisions could be a viable option, leaving a gradual transition to hard law provisions in the future.

8. Considering the differences in the level of development, technical level, and regulatory capabilities of the participants, some participants proposed that the negotiations should adopt a flexible commitment framework. Japan suggested a two-tier approach to e-commerce commitments with some members taking deep commitments and other taking shallower commitments. The EU has advocated the adoption of an *à la carte* negotiation framework to adapt to the demands of different participants, who would be able to choose the provisions they are willing to accept. The two-tier approach might be more conducive to maintaining the relative unity of the negotiation framework and facilitate the parties to reach an agreement.

9. Any agreement should include technical assistance provisions to effectively address the concerns of the developing countries and LDCs on the implementation capacity, so that more WTO members could join the agreement.[36] These countries could be supported in the formulation of relevant domestic laws and regulations and the establishment of law enforcement agencies to implement e-commerce provisions, such as electronic signatures and certification, paperless trade, online consumer protection, and personal information protection.

10. The agreement should promote predictability by clarifying the coverage of the exceptions, including by offering a definition of what constitutes a legitimate policy objective and an essential security interest. If anything, members should have the possibility to discuss how a certain measure is expected to achieve a specific policy objective and provide information of possible alternatives which are less trade restrictive. This dialogue would also be greatly enriched by the contribution of regulatory authorities, practitioners, academics, and private sector representatives.

11. The system agreed should try to accommodate future developments. One reason for ITA's success in meeting technological changes is the use of narrative definitions of products, for which it was not possible to identify the HS code.[37] Similarly, members of the negotiations on e-commerce should seek similar approaches to clarify the coverage of the commitments, for example by endorsement classification tools, such as the Understanding on Computer and Related Services (S/CSC/W/51), which clarify the sectoral coverage of services commitments.

The WTO e-commerce negotiations cover a significant portion of the WTO membership, and it is expected that more members will continue to join, providing a unique opportunity for building e-commerce rules in the 21st century. Bridging the gaps in the positions of the participants and finding a compromise which is open, inclusive and facilitates the participation of the least developed members would help to revive the WTO's relevance for the 21st century global economy.

REFERENCES

Azmeh, S, C G Foster, & J Echavarri (2020), 'The International Trade Regime and the Quest for Free Digital Trade', *International Studies Review*, 22(3): 671–692.

Baker, A S, P Lichtenbaum, M D Shenk, and M S Yeo (2001), 'E-Products and the WTO', *International Lawyer* 35: 5-7.

36 The WTO Trade Facilitation Agreement was the first agreement in the history of the multilateral trading system to include technical assistance clauses and stipulates that 'donor members agree to facilitate the provision of assistance and support for capacity building to developing country and least-developed country Members on mutually agreed terms either bilaterally or through the appropriate international organizations'.

37 Harmonized Commodity Description and Coding System.

Bergemann, K L (2002), 'A Digital Free Trade Zone and Necessarily-Regulated Self-Governance for Electronic Commerce: The World Trade Organization, International Law, and Classical Liberalism in Cyberspace', *Marshall Journal of Computer and Information Law* 20: 595-601.

Burri, M and R Polanco (2020), 'Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset', *Journal of International Economic Law* 23(1): 187–220, https://doi.org/10.1093/jiel/jgz044.

CNNum (2017), 'Strengthening EU's Negotiation Strategy to Make TTIP a Sustainable Blueprint for the Digital Economy and Society: Opinion of the French Digital Council', French Digital Council.

European Commission (2018), 'Questions & Answers on the Japan adequacy decision', MEMO/18/4503, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4503.

EPRS (2020a), 'Digital sovereignty for Europe', EPRS Ideas Paper: Towards a more resilient EU, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

EPRS (2020b), 'WTO e-commerce negotiations', At a Glance, European Parliamentary ResearchService,https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/659263/EPRS_ATA(2020)659263_EN.pdf.

Friends of E-Commerce for Development (2017), 'Developing countries launch roadmap for international trade and development policy' (Press release): https://www.ip-watch.org/weblog/wp-content/uploads/2017/04/Press-Release-FED-MinisterialMeeting-25.04.17-002.pdf.

López González, J & J Ferencz (2018), 'Digital trade and market openness', OECD Trade Policy Papers, No. 217: http://dx.doi.org/10.1787/1bd89c9a-en.

MIKTA (2016), MIKTA e-commerce workshop reflections, http://www.mikta.org/document/others.php?at=view&idx=235&ckattempt=1.

Ismail, Y (2020), 'E-commerce in the World Trade Organization: History and latest developments in the negotiations under the Joint Statement', International Institute for Sustainable Development and CUTS International, https://www.iisd.org/sites/default/files/publications/e-commerce-worldtrade-organization-.pdf.

Leblond, P (2020), 'Digital Trade: Is RCEP the WTO's future?', Centre for International Governance Innovation.

Micallef, J A (2019), 'Digital Trade in EU FTAs: Are EU FTAs Allowing Cross Border Digital Trade to Reach Its Full Potential?', *Journal of World Trade* 53(5): 855-870, https://kluwerlawonline.com/journalarticle/Journal+of+World+Trade/53.5/TRAD2019034.

WTO (1998a), 'Declaration on Global Electronic Commerce', adopted on 20 May 1998, Ministerial Conference Second Session, WT/MIN(98)/DEC/2.

WTO (1998b), 'Work Programme on Electronic Commerce', adopted by the General Council on 25 September 1998, WT/L/274.

WTO (2011a), Work Programme on Electronic Commerce: Communication from the European Union and the United States, S/C/W/338.

WTO (2011b), Work Programme on Electronic Commerce: Communication from the United States: Ensuring that Trade Rules Support Innovative Advances in Computer Applications and platforms, such as Mobile Applications and the Provision of Cloud Computing Services, S/C/W/339.

WTO (2014), Work Programme on Electronic Commerce: Communication from the United States, S/C/W/359.

WTO (2015), Nairobi Ministerial Declaration, WT/MIN(15)/DEC.

WTO (2016), Working programme on electronic commerce: Non-paper from the United States, JOB/GC/94.

WTO (2017a), 20 Years of the Information Technology Agreement https://www.wto.org/english/res_e/booksp_e/ita20years_2017_chap2_e.pdf.

WTO (2017b), Joint Statement on Electronic Commerce, WT/MIN(17)/60.

WTO (2017c), Working programme on e-commerce, Statement by the Africa Group, WT/MIN(17)/21.

WTO (2019a), Joint statement on electronic commerce: Communication from Côte D'ivoire, INF/ECOM/49.

WTO (2019b), Communication from China, Joint Statement on Electronic Commerce, INF/ECOM/19.

WTO (2020), Joint Statement Initiative On E-commerce: Co-conveners' Update, https://www.wto.org/english/news_e/news20_e/ecom_14dec20_e.pdf.

Wu, M (2017), *Digital trade-related provisions in regional trade agreements: Existing models and lessons for the multilateral trade system*, ICTSD.

Yakovleva, Sand K Irion (2020), 'Pitching trade against privacy: reconciling EU governance of personal data flows with external trade', *International Data Privacy Law*, 10(3): 201-221.

ABOUT THE AUTHORS

Martina F. Ferracane is a Post-Doctoral Researcher focusing on digital trade and data flows at the European University Institute and she acts regularly as a consultant for several organizations including the UN, the WEF and the WB. Martina also manages FabLab Western Sicily, an NGO that brings creative digital education to Sicilian kids.

LI Mosi is a Research Professor at Shanghai University of International Business and Economics (SUIBE), China. She serves as an expert on the National Digital Trade Expert Working Group and National Informatization Expert Consultation Committee. She was a Visiting Scholar at Georgetown University Law Center in 2016-2017.