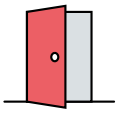
1 GLOBAL DATA TRANSMISSION AND LIABILITY FRAMEWORKS

Global data transmission is required:

- to realize trade activities (i.e. international provision of services, tracking international cargo across borders);
- to coordinate operations across global value chains (i.e. management of human resources, optimization of internal processes);
- to exchange trade-related information among supply chain stakeholders.

However, cross-border data flow can be limited by: (i) access to data transmission capacities at an affordable price, bandwidth and continuity as well as access to digital skills; and (ii) content regulation of data if regulatory fragmentation is not addressed through a global alignment on content and data regulation and on a liability framework. Global coordination will be required to ensure connectivity is fast and affordable, without compromising privacy, confidentiality and security.

A | DIGITAL INFRASTRUCTURE ENABLING GLOBAL DATA TRANSMISSION



With the growing number of connected devices, demand for broadband coverage keeps increasing (see Box 3). However, connectivity progresses at different paces around the world. The traditional digital divide between developed and developing countries in terms of internet connectivity, access and use remains high.

> **"The traditional digital divide between developed and developing countries in terms of internet connectivity, access and use remains high. While 90 per cent of the population in developed countries was using the internet in 2021, in least-developed countries it was only 27 per cent."**

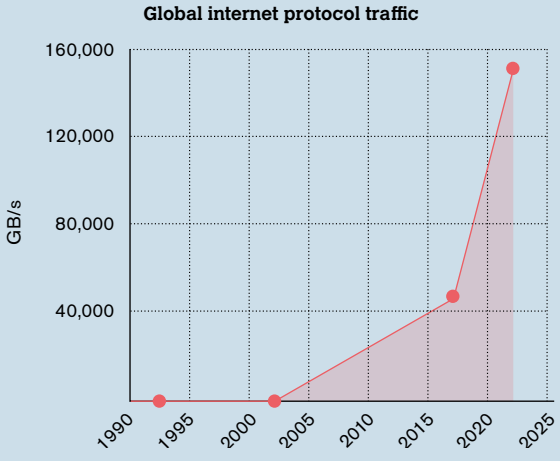
The most recent data of the International Telecommunication Union (ITU, 2021) estimates that 63 per cent of the world's population (4.9 billion people) were using the internet in 2021. While 90 per cent of the population in developed countries was using the internet in 2021, in least-developed countries it was only 27 per cent.

All countries experience a digital divide between urban and rural areas. While virtually all urban areas in the world are covered by mobile-broadband networks, there are many gaps in rural areas. The advent of 5G technology providing devices with broadband access might widen the digital divide, as devices using older generations, such as 3G, might not be able to access broadband.

BOX 3

INCREASED GLOBAL INTERNET TRAFFIC CALLS FOR A GLOBAL APPROACH TO DIGITAL CONNECTIVITY

Global internet protocol traffic, a proxy for data flows, has grown dramatically since 2000. From 100 gigabytes (GB) per day in 1992, 100 GB per second in 2002 to 46,000 GB per second in 2017, with global internet protocol traffic projected to reach 150,000 GB per second by 2022 (Cisco, 2018).* Demands for reliable and fast connections are expected to continue to increase given the growing number of IoT devices connected to the internet. One estimate suggests that the IoT will be made up of over 30 billion devices worldwide by 2025 (more than four objects per person), representing global growth of more than 150 per cent over five years since 2020.**



* *Source:* World Bank calculations and Cisco (2018). See https://wdr2021.worldbank.org/stories/crossing-borders.

** See https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide.

> "Trade contributes to the transfer of technologies across borders and helps to bridge the digital divide."

High costs for internet access relative to income remain one of the main barriers to the use of ICT services worldwide. The average cost of a mobile-data basket of 1.5 GB in developing countries, least-developed countries, landlocked developing countries and small island developing States is substantially above 2 per cent of monthly gross national income per capita (target set by the Broadband Commission for Sustainable Development for 2025). In addition to affordability, the effective use of the internet can be hindered by factors such as:

- low level of education;
- lack of relevant content and in the local language;
- lack of digital skills;
- low-quality internet connection.

Strengthening competition in developing countries could increase the quality of international bandwidth. The ITU[1] reports that:

> "This challenge is compounded by the fact that some developing countries, and even whole regions, are not yet served by undersea communications cables, forcing them to rely on higher priced satellite access. The costing issue is exacerbated if the international gateway that carries IP data to other countries is available solely from a local incumbent monopoly that faces no competition on rates. … Consequently, prices tend to remain high."

What can trade agreements do to help alleviate the digital divide in terms of infrastructure?

Trade agreements have contributed to the far-reaching changes of the telecommunications market, both hardware and software, since 2010. Multilateral, plurilateral and regional efforts highlighted in the following subsections should be further pursued by governments to foster global connectivity for all. Trade, through all its forms, including foreign direct investment, can increase competition, driving down connectivity costs and increasing quality. Trade also contributes to the transfer of technologies across borders, thus helping to bridge the digital divide. Some trade agreements have made substantial contributions.

Market access commitments in telecommunications services

Over 120 WTO members have made commitments to open markets in telecommunications services, most of which apply to basic services such as fixed and mobile telephony and real-time data transmission. These commitments comprise guarantees regarding, for instance, the establishment of new telecommunications companies, foreign direct investment in existing companies and cross-border transmission of telecommunications services. However, many trade restrictions persist in telecommunication services (see Table 1) and procedures often remain complex and paper intensive (e.g. the number of documents needed to obtain a business permit ranges from two to 19). Further market access commitments could reduce these barriers.

Competition in telecommunications services sectors

Over 100 WTO members have committed to the regulatory principles spelled out in the Reference Paper distributed in 1996 by the Negotiating Group on Basic Telecommunications.[2] The competitive safeguards therein guarantee that data transmission services providers may interconnect their systems on reasonable and non-discriminatory terms in a regulatory environment that is impartial and transparent, thereby supporting the development of transmission networks in a territory and largely reflecting best practice in telecommunications regulation. Competition is a key driver to investment and, in turn, to bandwidth at an affordable price.

As another venue to foster competition, some RTAs have introduced competition safeguards with respect to internet access providers (e.g. SADEA) or to operators controlling international submarine cable systems (e.g. Comprehensive and Progressive Agreement for Trans-Pacific Partnership), thereby supporting interconnection on non-discriminatory and commercial terms. To stimulate connectivity infrastructure development, SADEA introduces transparency obligations and streamlines procedures for permits needed for the installation, maintenance or repair of submarine cable systems. At the WTO, members participating in the Joint Initiative on E-commerce are also discussing a possible revision of the WTO Reference Paper to include all telecommunications and internet access services.[3]

Net neutrality

Most recent RTAs have introduced a net neutrality principle to ensure that internet service providers treat

TABLE 1

ACCESS BARRIERS TO THE TELECOMMUNICATIONS SECTOR

Barrier description	Number of governments with such a barrier
There are limits to the proportion of shares that can be acquired by foreign investors in publicly controlled firms	18
Acquisition and use of land and real estate by foreigners is restricted	32
Quotas on independent services suppliers	10
Labour market tests for intra-corporate transferees	36
Labour market tests for contractual services suppliers	34
Public procurement: explicit preferences for local suppliers	23
Public procurement: thresholds above which tender is mandated conditions of competition in favour of local firms	20
National, state or provincial government control of at least one major firm in the sector	22

Source: Organisation for Economic Co-operation and Development (OECD) Digital Services Trade Restrictiveness Index database.

all data transmission equally. This outcome elaborates on the Annex on Telecommunications[4] contained in the General Agreement on Trade in Services (GATS), which states in Article 5 that:

> "(a) Each Member shall ensure that any service supplier of any other Member is accorded access to and use of public telecommunications transport networks and services on reasonable and non-discriminatory terms and conditions, for the supply of a service".

Systematically including net neutrality in trade agreements would help to ensure that the internet users access the internet on reasonable and non-discriminatory terms.

WTO's Information Technology Agreement

Initially signed by 29 WTO members in 1996, the ITA has contributed to the elimination of tariffs on IT products and covers 97 per cent of world trade in IT products (WTO, 2017). In 2015, over 50 WTO members concluded the expansion of the ITA, which now covers an additional 201 products. In 2020, world exports of both ITA and ITA Expansion products accounted for more than 20 per cent of global exports of manufactured products.[5]

Small businesses have a lot to gain from greater ICT access thanks to the ITA, as they see their competitiveness boosted and their chances to access the international market improved. Ezell and Wu (2017) report "that ICT-enabled firms in developing countries were twice as profitable, 65 percent more productive, and boosting employment 25 percent faster than firms that did not adopt ICTs."

This plurilateral agreement and the expansion are open to all WTO members, and several are looking into joining. In July 2021, the Lao People's Democratic Republic announced that they would join the ITA and the expansion, becoming the first least-developed country to accede to both of these agreements.[6]

It is important to note that market access gains from tariff liberalization may become meaningless if they are undermined by discriminatory or unnecessary NTMs. Simplifying and streamlining NTMs, such as conformity assessment procedures or labelling for IT products, should therefore be a key objective along with tariff liberalization.

Regulatory coherence and cooperation with regard to cybersecurity rules

There has been a recent increase in notified technical barriers to trade (TBT) measures dealing with the cybersecurity of IoT, 5G technology, 3D printing devices, drones and autonomous vehicles, which address potential abuses on the basis of public safety and national security, safety and performance of 5G products, and interoperability (Hoe Lim, 2021).

To improve the cybersecurity of equipment, infrastructure, and software-enabled and network-connected goods, governments rely to a large extent on certification and labelling schemes. While regulatory approaches to cybersecurity certification are generally envisioned as voluntary, there is an early trend in which schemes and corresponding requirements may become mandatory. Divergent regulatory approaches may hinder the transfer of technologies and thereby preventing the digital divide to narrow.

The TBT Agreement promotes global regulatory coherence (via sharing and discussing international standards at the pre-implementation stage) and global regulatory cooperation (via good regulatory practices, equivalence and mutual recognition). However, compared to other regulatory areas such as cybersecurity, international standards are often complemented by national regulations and standards, thus sustaining regulatory fragmentation.

Trade agreements could encourage the use and development of international standards and mutual recognition schemes, such as the Common Criteria (see Box 4), to foster regulatory convergence. Interoperability between international standards should also be considered. Like regulatory fragmentation, non-interoperable international standards will increase audit and compliance costs for companies.

The WTO Principles for the Development of International Standards, Guides and Recommendations aim to avoid conflicting standards.[7] The six principles were agreed upon by the TBT Committee in 2000 to provide guidance for WTO members when developing international standards:

1. transparency
2. openness
3. impartiality and consensus
4. effectiveness and relevance
5. coherence
6. development dimension

BOX 4

COMMON CRITERIA

The Common Criteria provides technical guidance for cybersecurity certification schemes of ICT products and systems. It is supported by the Common Methodology for Information Technology Security Evaluation (CEM), which describes how evaluations and assessments should be conducted. The Common Criteria Recognition Arrangement (CCRA) ensures mutual acceptance of security certificates internationally. IT products which earn a Common Criteria certificate can be procured or used without the need for further evaluation. In turn, these international standards contribute significantly to confidence in the security of IT products internationally. The CCRA was signed in 1998 and now has 31 parties.

At the regional level, an equivalent mutual recognition agreement (MRA) was signed in 1998: the Senior Officials Group Information Systems Security (SOG-IS) MRA includes 15 EU and EFTA member States.

Although these principles were adopted in the context of the TBT Agreement, which is concerned with trade in goods, they are relevant to international standards on digital trade in services. The six principles have become so widely accepted by WTO members not only multilaterally but also regionally, that a growing number of RTAs not only incorporate the six principles in their TBT chapters, but also make them mandatory (McDaniels *et al.*, 2018).

Some international standardizing bodies have also embraced these principles, such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

"Although the six Principles for the Development of International Standards, Guides and Recommendations were adopted in the context of the TBT Agreement, which is concerned with trade in goods, they are relevant to international standards on digital trade in services."

Using the TBT Committee to address trade concerns relating to cybersecurity rules could help to solve them without escalating them into WTO formal disputes, ultimately solving these issues more promptly for the sake of technology transfer and the closing of the digital divide.

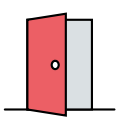
Transfer of technology

A number of provisions in WTO agreements refer to the need for a transfer of technology to take place between developed and developing country members. However, the modalities of such transfers are not specified. For instance, the WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) aims to achieve the transfer and dissemination of technology as part of its objectives, and specifically requires developed country members to provide incentives for their companies to promote the transfer of technology to least-developed countries. Similarly, Article 6 of the Annex on Telecommunications in GATS states:

> "(d) Members shall give special consideration to opportunities for the least-developed countries to encourage foreign suppliers of telecommunications services to assist in the transfer of technology, training and other activities that support the development of their telecommunications infrastructure and expansion of their telecommunications services trade."

These provisions should be fully operationalized, and trade agreements could specify these modalities. Best practices on incentives aiming at closing the digital divide could be shared in the WTO Working Group on Transfer of Technology.[8]

B | GLOBAL ALIGNMENT ON CONTENT REGULATION OF DATA AND ON LIABILITY FRAMEWORKS TO SUPPORT CROSS-BORDER DATA FLOWS



The second source of obstacles to cross-border data flows is regulatory measures concerning the content of data (i.e. the actual information transmitted). The content of data can be personal, sensitive or confidential and can expose individuals and organizations to risks such as, *inter alia*: unauthorized access to and use of personal and business confidential information or a device connected to the internet; cyberthreats to critical infrastructure and information; a loss of connectivity; or price discrimination based on personal information.

Many incidents relate to cyber vulnerabilities, although some malicious cyberthreats can also affect companies through direct hacking (see Box 5) or by targeting an organization in its supply chain. As the number of people and machines communicating online increases, the likelihood of data-related risks and the severity of

BOX 5

HOW HACKING OR CYBER VULNERABILITIES CAN AFFECT INTERNATIONAL TRADE

Under an electronic release system, carriers provide, against bills of lading, computer-generated pin codes, which are sent in a release note via email to the receivers of their agents and the port terminal to take delivery of the goods.

Upon arrival, when an attempt is made to collect the containers, it is discovered that two of them have already been collected by unauthorized persons. It is not clear how the thieves accessed the codes – either from the recipient's or the sender's IT infrastructure.

Note: See the 2017 case from the England and Wales Court of Appeal between MSC Mediterranean Shipping Company and Glencore ([2017] EWCA Civ 365).

> "The different levels of cybermaturity of companies and economies need to be addressed to support the global adoption and scalability of TradeTech."

their consequences will also increase, especially for small businesses, who are the most vulnerable.

In the digital world, the vulnerabilities of one company impact the other companies sharing information in the same supply chain. More generally, the vulnerabilities of one economy might prevent foreign companies from offering their technologies to stakeholders in that economy. These different levels of cybermaturity of companies and economies need to be addressed to support the global adoption and scalability of TradeTech. Cybersecurity needs to be dealt with as if it were a global public good.

Advanced technologies make the application of data protection laws more difficult. For instance, identifying data controllers and data processors[9] can be very challenging in permissionless blockchain-based systems. Arguably, participants entering personal data in blocks of the ledger may be regarded as controllers of the data they provided or to which they have access through the system; unless they act as the technology service provider supporting the system, in which case they are likely to be characterized as a data processor.

As jurisdictions respond to these threats unilaterally, regulatory fragmentation could hinder global data transmission and ultimately affect market access for companies relying on data moving across borders. For consumers, this could result in fewer products, higher prices and lower quality (see Box 6).

How are governments dealing with content and data regulation while safeguarding cross-border data flows and legitimate objectives?

Many governments have introduced laws and regulations to mitigate these types of data-related risk, including personal data protection measures, cross-border data measures, product safety measures and cybersecurity measures. Regulatory fragmentation can create uncertainty for consumers and supply chain actors as to whether and how they can access remedies abroad and upon which liability framework they can rely (see Box 7).

Some laws and regulations apply across many sectors, such as the EU General Data Protection Regulation or the Cybersecurity Law of China relating to critical infrastructure sectors. Other laws are applicable to particular sectors or technologies, such regulations on AI, autonomous vehicles and drones.

Some measures use a risk-based approach, whereas others use a prescriptive approach. According to cybersecurity experts, given the evolving nature of cybersecurity threats, a risk-based approach may be more effective. Addressing cybersecurity in ICT by product-specific regulation might not be warranted, since any developments in technology would make such regulations obsolete very quickly (National Board of Trade Sweden, 2018). Risk-based regulatory approaches might be beneficial for companies (in particular small businesses) because it avoids disproportionate burdens. Indeed, the smaller the firm, the heavier the burden of compliance.

To regulate AI that uses personal data, some governments have adopted a risk-based approach. The European Commission proposes an ex-ante conformity assessment framework that would require firms to validate that their AI products and services adhere to certain EU-specific requirements before offering them on the EU market or putting them into service.

What can trade agreements do to foster content regulation of data that supports trusted cross-border data flows?

Different channels have been used from a trade policy perspective to support global data transmissions, but there remain unseized opportunities.

Regulatory convergence

Trade agreements play a key role in fostering regulatory convergence on flows of data. Some 105 RTAs call on governments to introduce domestic frameworks for personal data protection, of which 47 require governments to take into account international standards.[10] Similarly, many RTAs have cybersecurity provisions encouraging governments to strengthen cybersecurity capabilities and to support international cooperation. However, there remain many unseized opportunities.

BOX 6

DATA REQUIREMENTS BARRING ENTRY INTO NEW MARKETS

Dorae* offers a flexible software system to its customers to digitize trade documents, automate processes, and track the origin of raw materials and the manufacturing steps. Customers define which data they enter into the system, without any review by Dorae. For security and customer convenience, Dorae's system is cloud-based, with infrastructure in commercial data centres around the world.

As part of its growth strategy, Dorae assessed entry into a new market. A large part of which focused on data localization requirements in the target market. These required that certain types of data be stored in a specific manner and not be transmitted across borders due to security concerns.

Since customers define the data they enter into the system, Dorae could not be 100 per cent certain that proscribed information would not be handled. Yet, they would still be liable for any infringement.

To mitigate the risk, Dorae could: curtail functionality such as information sharing between customers; build additional infrastructure; or change local terms and conditions. However, these solutions were either incomplete, expensive or resulted in a reduced user experience incompatible with Dorae's reputation and product quality.

Dorae concluded that the upfront costs and unmeasurable legal risks outweighed the near-term growth prospects, so market entrance was put on hold. This was not just a missed trade opportunity for the company, but a missed opportunity for supply chain stakeholders that might have benefited from supply chains with greater visibility and transparency.

* See https://www.dorae.com.

BOX 7

LIABILITY

The ability to identify uniquely and without ambiguity the person liable for any damage is essential to guarantee access to remedies. Ideally, the transfer of responsibility must be facilitated whichever digital solution is used.

Due to the opacity, connectivity and autonomy of AI systems, which can involve several (often cross-border) complex contractual arrangements with many actors, determining who is liable by tracing back harmful actions of AI systems to a human input or design aspect is extremely difficult. Moreover, many machine learning models use incremental learning systems that are uninterpretable to humans, and existing regulation does not sufficiently address the dynamic nature of these machine learning models, which could be said to have "a mind of their own".

Another issue concerns potential glitches in or between the programming language and the executable machine code, which could lead to the code not doing what it was intended to do when executed. Arguably, the risk of a glitch exists in any computer program. The main challenge in ascertaining liability in (permissionless) blockchain systems is the difficulty in determining the relationship between the many parties involved: (i) the core group, which sets up the code design; (ii) the owners of additional servers running the DLT code for validation purposes; (iii) users of the DLT; and (iv) third parties affected by the system without directly relying on the technology.

Typically in permissionless blockchains, node owners will not even know who operates the other nodes. Consequently, there may be challenges in identifying a potential defendant from whom legal redress can be sought, let alone the actual identity. By contrast, permissioned blockchains have their own rulebook that defines liabilities. This poses problems, however, as different blockchain and DLT platforms may follow different approaches, which can affect interoperability. Clarifying these issues may be needed to support the wider adoption of blockchain and DLT in trade.

Many non-contractual liabilities may potentially arise with transactions through smart contracts (e.g. claims for fraud, unfair trade practices, insider trading, market abuse), which could be an area of risk of interest to insurance companies. However, conditions under which such insurance applies will be tricky to draft.

TradeTech will require existing liability frameworks to be adapted or new frameworks to be developed. Such initiatives should be coordinated globally to avoid regulatory fragmentation, trade barriers and consumer distrust. In that respect, some governments have considered extending their current domestic product liability and safety framework to software-enabled or network-connected goods. Clarifying the scope of product liability and safety frameworks with respect to IoT would provide consumers with more protection and greater legal certainty.

> **"Trade agreements play a key role in fostering regulatory convergence on flows of data."**

With regard to privacy rules, the general approach to regulate cross-border data flows is to ensure an adequate level of data protection in two or more territories. Regulatory cooperation between some governments has led to the introduction of equivalence schemes (e.g. adequacy decisions) and regional certification systems (e.g. Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules System) to establish this equivalent level of protection, but these mechanisms remain limited in scope. Further international regulatory cooperation is needed to make them truly global.

Only a few RTAs facilitate the interoperability between cross-border data flow mechanisms. For example, Article 19.8 of the United States–Mexico–Canada Agreement refers explicitly to the APEC Cross-Border Privacy Rules System and recognizes it as "a valid mechanism to facilitate cross-border information transfers while protecting personal information." Article 4.2(10) of DEPA also encourages its signing parties to mutually recognize the other parties' data protection with the exact same wording in. Systemically supporting these mechanisms in trade agreements can help companies to become aware of their existence and to use them. Coordination at the multilateral level will be needed to prevent data transfer mechanisms from landing in silos.

The Osaka Track is a major international initiative on data flows, which was launched by heads of governments under Japan's G20 leadership in 2019. The framework "data free flow with trust" – the key underlying concept of the Osaka Track – maps a multidimensional architecture for international cooperation on data flows, between governments, as well as involving business, with recommendations to increase levels of governance trust and to build openness through trade rules and other tools (World Economic Forum, 2020b).

With respect to rules on AI, nascent international guidelines also intend to foster regulatory coherence, for instance:

- OECD principles on AI (OECD, 2022);
- G20 New Industrial Revolution Action Plan;
- G20's joint statement on human-centred AI and subsequent endorsement of the OECD principles on AI in the G20 Ministerial Statement on Trade and Digital Economy, June 2019;
- G7 Global Partnership on Artificial Intelligence (GPAI);
- Council of Europe Committee of Experts on human rights dimensions of automated data processing and different forms of artificial intelligence;
- Standardization in the area of AI by the ISO/IEC joint technical committee.

As governments fund AI development, it would be useful for some of it to be dedicated to interoperability. Only a few trade agreements, such as DEPA, include provisions in which the parties acknowledge the benefits of developing mutual understanding and ultimately ensuring that (see paragraphs 2 and 4 of Article 8):

> "ethical and governance frameworks for the trusted, safe and responsible use of AI technologies … are internationally aligned, in order to facilitate, as far as possible, the adoption and use of AI technologies across the Parties' respective jurisdictions … [and] … endeavour to take into consideration internationally recognised principles or guidelines, including explainability, transparency, fairness and human-centred values."

Trade agreements could promote international guidelines on AI governance before witnessing a national or regional silo-approach to AI regulation. Regulatory convergence would support the global adoption and use of AI technologies in trade. Otherwise, regulatory fragmentation will lead to more barriers.[11]

Cybersecurity cooperation and data exchange between governments for law enforcement and regulatory oversight

Before trade agreements include cybersecurity cooperation to address borderless threats, several key issues are still to be addressed. Around 50 RTAs contain rules that encourage capacity-building of national entities responsible for computer security incident response (CSIR) and workforce development through mutual recognition of qualifications, as well as the cross-border exchange of information to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks globally. However, these provisions focus on CSIR entities, thus disregarding the exchange of information between other governmental bodies, such as between law enforcement authorities. Provisions on cybersecurity are also being discussed in the context of the WTO Joint Initiative on E-commerce.

Cybersecurity cooperation should aim at closing the gap in cybersecurity capabilities of economies and companies. Given the difference in information assets and the knowledge and infrastructure used to protect them, some economies and companies are more vulnerable than others, which undermines internet reliability across borders. Building preventive capacities, rather than just being reactive to cyberattacks, is key to fostering cross-border reliability and to guaranteeing that regulatory responses (e.g. certification requirements) are enforced. There is little use in preparing, adopting and implementing (often complex and costly) regulatory responses unless there are effective enforcement processes in place. Trade agreements should encourage governments to strengthen enforcement capacities of stakeholders with cybersecurity responsibilities.

No trade agreement addresses the inefficiency of mutual legal assistance procedures. The long review process featured in mutual legal assistance treaties (MLATs) often defeats the purpose of data requests through this mechanism, as law enforcement agencies are unable to secure critical evidence within an appropriate time frame. As a result, some governments have turned to data localization measures as a way to expedite such access by reducing the reliance of the government of the localizing country on the foreign government in whose jurisdiction the relevant data are stored. To limit the proliferation of such measures, it is imperative for policymakers and other stakeholders to recognize the need for a more effective and efficient international data-sharing regime for law enforcement purposes than existing MLATs. To facilitate timely data exchange between governmental bodies for law enforcement purposes, trade negotiators could leverage the political momentum created by the negotiation of trade agreements to reform MLATs. In addition, trade agreements could authorize or encourage regulators to directly exchange e-documents among themselves rather than relying on the MLAT process.

Some countries are exploring alternative solutions unilaterally, which trade agreements could discuss, and potentially leverage – preferably at the multilateral level. One approach to facilitate government access to data for law enforcement purposes is the Kingdom of Bahrain's Legislative Decree No. 56 of 2018, In Respect of Providing Cloud Computing Services to Foreign Parties. With this law, data stored in data centres in the Kingdom of Bahrain are subject to the domestic law of the State where a consumer resides (or is incorporated in cases of legal persons) and are thereby subject to the jurisdiction of that State's courts and other competent authorities.

Collaboration and competition in data-driven markets

Cross-border data flows can also be hindered by some oligopolistic tendencies, which create customer lock-in for data services. Although data are generated across different markets, in some cases it is mainly stored, processed and commercially exploited in only a few regions. Choice and competition are key to ensuring that no single person, company, country or region controls important infrastructural digital components and the digitalization of global trade.

Around 40 RTAs agree to explore adequate approaches to promoting and protecting competition in digital markets and to strengthen collaboration mechanisms for identifying and mitigating market distortions arising from abuse of market dominance. However, only one RTA has so far explored solutions to address data services lock-ins. Paragraph 3 of Article 9.4 of DEPA encourages parties "to collaborate on data-sharing projects and mechanisms, and proof of concepts for new uses of data, including data sandboxes, to promote data-driven innovation." The issue of competition in digital markets is also being discussed in the context of the WTO Joint Initiative on E-commerce.

There are other governmental initiatives which could be leveraged by trade agreements, such as the cross-border regulatory sandbox between Abu Dhabi Global Market (ADGM) and the Association of Southeast Asian Nations (ASEAN) Financial Innovation Network, where start-ups and financial bodies can experiment with technologies and ideas while sharing data in a predictable and regulated environment, or the regulatory sandbox between ASEAN and ICT ministers whereby businesses can test their services without breaking data privacy rules or facing regulatory sanctions. Trade agreements could encourage governments to exchange best practices on existing data-sharing mechanisms and on how best to address related legal and technical challenges.

Coherent regulatory processes

Bilateral and international coordination across government agencies for the design and implementation of data governance regulation helps to foster regulatory coherence and thereby global data transmission. Uncoordinated regulation between these authorities not only creates legal complexity but also can unintentionally undermine the economic opportunities associated with data.

For instance, an approach to personal data protection that makes compliance difficult and costly can reduce

BOX 8

THE IMPACT OF DATA AND CONTENT REGULATION ON OCEAN SHIPPING VISIBILITY

Information on cargo volumes and positions enables traders to optimize logistics by predicting congestion and choosing shipping routes accordingly. Due to the COVID-19 pandemic, the surge in demand for goods and shortage of containers have created port disruptions around the world, making shipping data even more important to determine schedule times for shipments.

New regulations put in place in certain jurisdictions have led domestic providers of these jurisdictions to stop providing shipping information to foreign companies, thereby significantly impacting ocean shipping visibility.

Source: Saul and Baptista (2021).

the value of data sharing, such as in the delivery of cross-border services or the tracking of shipments, containers and products across supply chains (see Box 8). Similarly, governmental bodies working in the regulatory field of cybersecurity generally focus on safety, security and resilience of critical assets and infrastructure, and are not necessarily aware of the implications on openness, interoperability and trade. Like other digital economy policy and regulatory initiatives, data regulation needs to be designed in collaboration with multiple stakeholders, including trade policymakers.

Trade agreements could encourage governments to foster dialogue between their regulatory bodies and trade policymakers and to encourage the exchange of good regulatory practice. This would help to: (i) set a common vision; (ii) enhance coherent implementation and coordination; (iii) deliver value from data; and (iv) lower trade costs. This is especially important where there are several regulators pursuing data regulation, which could inadvertently result in new obstacles to trade.

ENDNOTES

1. See https://www.itu.int/en/ITU-T/studygroups/2013-2016/03/Pages/iic.aspx.
2. The Reference Paper is a set of regulatory principles that is legally binding for those WTO members which have committed to it by appending the document, in whole or in part, to their schedules of commitments. See https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm.
3. See https://www.wto.org/english/news_e/news21_e/ecom_20apr21_e.htm.
4. The Annex on Telecommunications concerns public telecommunications transport networks and services: transport services refer to data transmission services; public refers to those telecommunications transport services that are required to be offered to the public generally. It refers to the ownership of a company.
5. See https://www.wto.org/english/news_e/news21_e/ita_02dec21_e.htm.
6. See https://www.wto.org/english/news_e/news21_e/ita_30jul21_e.htm.
7. See https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm.
8. See https://www.wto.org/english/tratop_e/devel_e/dev_wkgp_trade_transfer_technology_e.htm.
9. The definitions of data controllers and data processors vary across jurisdictions. Here, the terms should be understood in the context of the EU General Data Protection Regulation.
10. TAPED dataset dated 25/01/2022, available at https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped.
11. Some argue, for example, that the EU proposal for an ex-ante conformity assessment framework could become a barrier to AI-based digital trade even if the products are safely and effectively used in other jurisdictions (World Economic Forum, 2020a).