Digital Trade and Data Protection: The Need for a Global Approach Balancing Policy Objectives

Habib Kazzi
Professor of International Economic Law, Lebanese University
MENA Legal Consultant
Lawyer at the Paris Bar Association

Abstract

In an increasingly data-driven global economy, this contribution analyses the ambiguous relationships between global trade, cross-border data flows, and online privacy. Free data flows and localization constitutes an essential driver for E-commerce and a pre-condition for its potential success. But legal and cultural differences between national, regional and international regimes on privacy and data protection, as well as variable public policy objectives pursued by governments, may constitute a new generation of non-tariff barriers to digital trade. This assessment makes more necessary a global approach balancing policy objectives, while enabling interoperability between differing national regimes and removing discriminatory trade barriers to cross-border data flows. For this purpose, any national privacy policy or international agreement should be based on the following three pillars: 1) adopting data protection principles and standards in accordance with OECD Privacy Guidelines; 2) setting up effective mechanisms for cooperation between national data protection commissions or authorities; and 3) providing for a "trade test" that ensures free flows and localization of data between countries, while recognizing that sometimes measures are necessary to achieve legitimate policy objectives and, in this case, such measures should be the least trade restrictive, non-discriminatory, and transparent.

Keywords: Digital Trade, Data Flows, Privacy, Public Policy Objectives, OECD Privacy Guidelines, WTO Principles.

Introduction

Trade policy, cross-border data flows, and online privacy have interrelated and ambiguous relationships. The rise of E-commerce raises challenges for States and citizens, notably through securing transactions; digital taxation and the processing of personal data in the context of cross-border flows and data localization. Cross-border data flows underlie today's globally connected world and are essential to conducting international trade and commerce. Data flows enable companies and individuals to track global supply chains, transmit information for online communication, provide cross-border services, share research, and support technological innovation (CRS Report, 2020).

Data flows and transfers can take various forms: 1) Data flows supporting traditional international trade in goods and services (B2B and B2C); 2) Data flows that are a full component of international trade (creation of new players and innovative sectors); and 3) internal corporate data flows through supply chain or human resources management. This might be information and communication of ideas exchanged

within the branches or subsidiaries of companies dispersed in several countries (Bughin and Lund, 2017).

Companies value consumers' personal online data for various reasons. Organizations may seek by way of illustration, to ease business transactions, collect and analyze marketing information and sales data, discover fraudulent payments, improve proprietary algorithms, detect disease patterns from medical histories, or develop competitive innovations. For some analysts, data should be comparedto oil or gold, but unlike those valuable substances, data is not a scarce resource; it can be analyzed, reused, shared, and combined with other information.

Nonetheless, while cross-border data flowsfoster innovation and increase productivity, the digital environment raises privacy and security challenges around information collected, stored and transmitted across the globe. Personal data is considered personal private property. Individuals often want to control who accesses their data and how it is used. Experts suggest that data may therefore be considered both a benefit and a liability that organizations hold. Data has value, but organizations take on risk by collecting personal data; they become responsible for protecting users' privacy and not misusing the information. Data privacy concerns have become more urgent as "[…] *the amount of online information organizations collect and the level of global data flows continue to expand*" (CRS Report, 2020). Recent incidents of private information being shared or exposed have also heightened public awareness of the importance of high tech companies, and the risks posed to personal data stored online.

In this environment, divergent regulatory approaches and shortcomings of national privacy laws and policies do not unfortunately facilitate the emergence of potential global standards on privacy and cross-border data flows. While about 130 countries have adopted or are in the process of adopting national privacy regimes, there are no comprehensive multilateral rules specifically about privacy or cross-border data flows (Burri, 2017).

Countries vary in their privacy policies and laws, reflecting differing priorities, cultures, and legal structures (UNCTAD Secretariat, 2019). The United States has traditionally supported open data flows and has regulated privacy at a sectoral level to cover data, such as health records, rather than create a comprehensive policy. Other countries are developing data privacy policies that affect international trade as some governments or groups seek to limit data flows outside of an organization or across national borders for a number of reasons. Blocking international data flows may impede the ability of a firm to do business or of an individual to conduct a transaction, creating a form of trade protectionism. Recent research has evidenced "[…] *not only the economic gains from digital trade and international data flows, but also the real economic costs of restrictions on such flows*" (CRS Report, 2020).

On the international scene, major global players, such as the United States and the EU, have begun to address these issues in negotiating new and updated trade agreements. International economic forums and organizations such as the Asia-Pacific Economic Cooperation (APEC) forum and the Organization for Economic Co-operation and Development (OECD) have alsoprovided for non-binding international guidelines and best practices.

While the digital environment is raising a number of privacy challenges, privacy

protection frameworks are generally developed at the national level. Cross-border flows of personal data are raising the issue of interoperability of these frameworks. The risk of fragmentation of Internet and loss of confidence by consumers and businesses in digital transactions is indeed great. For many policymakers, the crux of the issue revolves around a double challenge: 1) developing a framework that protects privacy while promoting economic development; and 2) ensuring a sufficient level of international interoperability to prevent the privacy protection framework from inhibiting international trade.Implicitly, the interaction between international trade and the flow and localization of personal data refers to the fragile balance between trade policies with their marked liberalism and Internet governance.
To better understand what is at stake, the remaining article is organized as follows. Section I analyzes the interaction between digital trade and cross-border flows of data. Section II discusses current economic and political issues surrounding personal data collection, storage, processing and transfer. While Section III stresses the gaps of domestic and international regulatory frameworks and the risk of fragmentation of Internet, Section IV tackles current challenges by shaping a global approach balancing national policy objectives. Finally, Section V concludes.

I-Interaction between digital trade and cross-border data flows

The international trading system is facing three major challenges: regionalization particularly with the increasing of mega-regional trade agreements; global value chains that shuffle the cards in terms of production, distribution and supply chain management; and the rise of digital economy, especially the cross-border E-commerce. The digital economy is a powerful force for global economic growth. Electronic commerce is at the core of this shift, and represents the new wave of globalization after successive rounds of trade liberalization in goods, services, investments, capital and workers. Today, five biggest companies in the world are in the technology sector which uses, processes, and generates huge data collected from all over the world (Apple, Amazon, Alphabet (Google holding company), Microsoft, and Facebook).
Online platforms have gradually become one of the most important business models of the 21st century. These entities are traditionally divided into two types. "Innovation platforms" enable third-party firms to add complementary products and services to a core product or technology. Prominent examples include Google Android and Apple iPhone operating systems as well as Amazon Web Services. The other type, "transaction platforms" such asAmazon Marketplace, Airbnb, or Uber, enables the exchange of information, goods, or services. Five of the six most valuable firms in the world are built around these types of platforms. Such platforms generate the same level of annual revenues (about $4.5 billion) as their non-platform counterparts, but used half the number of employees. They also had twice the operating profits and much higher market values and growth rates (Yoffe, Gawer and Cusumano, 2019). With 90% of online research in the world for Google, and Facebook which has 2 billion active users (of which 900 million people have international connections), these two giants concentrate 70% of Web traffic, and therefore a large part of power and influence (Mckinsey Global Institute, 2016).

A more digitized globalization creates unprecedented opportunities to developing countries, small businesses and start-ups, and billions of people. Tens of millions of small and medium-sized businesses around the world have turned into exporters by joining e-commerce markets such as Alibaba, Amazon, eBay, Flipkart and Rakuten. Individuals use global digital platforms to learn, find work, showcase their talents and build personal networks, thus creating a more global marketplace.

According to the World Trade Organization (WTO), one of the most significant overall impacts of the growth of digital technologies is in transforming international trade. Technology can lower the costs of trade, change the types of goods and services that are traded, and may even change the factors defining a country's comparative advantage. The extent of the impact of digital technologies on trade, however, depends in large part on open cross-border data flows and free data localization (WTO, World Trade Report 2018).

Modern digital markets are fuelled by personal data. While almost 400 million people regularly participate in cross-border E-commerce, the latter is impossible without data flows and freedom of storage which accompany the trade of services and products. Cross-border data flows are part of, and integral to, digital trade and facilitate the movement of goods, services, people, and finance. They represent around 3.5% of total world GDP. Already half of the services exchanged in the world are digital, and 12% of the world trade of goods is conducted digitally, either B2C or B2B.Recent studies stressed that Cross-border data flows have increased 45 times since 2005, with predictable growth multiplied by nine over the next five years as information, research, communications, videos, transactions and intra-group traffic flows continue (Bughin and Lund, 2017).

Cross-border data flow networks are not traditional; the trade generated is thus:

- more global and balanced than physical trade with a center of gravity that moves from the U.S. and the EU to emerging and Asian countries;
- more inclusive with the participation of new State (developing economies) and private (SMEs and individuals) actors.
- Self-dynamic compared tophysical trade flows. Referring to the example of oil markets, some analysts are even going so far as to claim that a personal data marketplace possibility could become a reality sooner than we think (Sonmez, 2020).

Proponents of the free flow of data argue that international data flows are driving the digital economy and creating new jobs, innovation and economic growth. As a result, any restriction of these flows would slow down innovation, growth and development.

II-Rationale for Restricting Cross-Border Flows and Localization of Data

While almost all types of cross-border transactions have a digital component, this digital economy is increasingly based on international data flows and free localization. Personal data has become an essential pillar of international trade. Its flow and storage are the source of an economic war between States. Data is considered the new oil for trade in the 21st century. The business value of personal data indeed comes mainly from massive processing (big data or cloud) which crosses various sources (social

networks, even medical data or data from private actors). These technologies are even used in politics as revealed by recent notorious scandals in the US and around the world (Chang, 2018).

Cross-border data flows raise new challenges for all stakeholders in international trade. Data is now laying down the law… and the fortune of some multinational companies. Such companies use international networks to transfer data from one country to another, thereby gaining organizational efficiency and competitiveness. Such practices have raised States' concerns in two counts. Some States fear a loss of competitiveness of their companies which do not have access to critical consumer data. Other States fear that their national privacy and economic regulation policies will be circumvented when data leaves the territory under their jurisdiction to be transferred to other countries, where it will be subject to different laws and policies.

For companies, digital economy has imperatively changed business processes and organizational models on a large scale. But this shift entails other major impact. They are required to implement the appropriate technical and organizational measures to ensure a sufficient level of consumer protection with regard to the risks presented by the processing and storage of personal data to be protected. Meeting this challenge requires significant costs and expertise, and therefore the risk of losing global competitiveness.

To address these issues, priorities vary among countries, ranging from liberal policies in this area to an exacerbated state interventionism:

1) Some countries adopt data policies that regulate flows of personal data in order to protect privacy.
2) Some countries regulate cross-border transfers of data for audit purposes (administrative or judicial investigations and prosecutions). These countries may require access to data located abroad or request that at least one copy be kept in the territory.
3) Another reason for regulation is industrial policy. Policymakers want to ensure their industries benefit from the value generated by their citizens' data, thus stimulating local digital industries.

In this regard, the EU General Data Protection Regulation (GDPR) is serving as a tool, if not a weapon, in the arena of economic rivalry. Some claim that the GDPR is a real declaration of economic and political war in the literal sense of the word. For the first time, a European regulation provides for sanctions against companies located outside European territory, despite the rules of private international law. The aim is to make it clear to partners and businesses that it will no longer be possible to profit blithely from the European citizens' data without risking heavy sanctions. Instead of forcing global partners, like China or the US, which are still reluctant to legislate on this matter, the GDPR directly attacks companies by requiring European contractors to choose their providers on the basis of their compliance with the GDPR. The outcome is that some American companies have been recently forced to transfer their data centers to Europe so as to maintain their market shares (Greenleaf, 2019).

4) Still another important reason for restrictions on data flows is national security, giving rise to data categorizations like 'important' or 'strategic' data that are mandated to remain locally.

5) Last but not least, in some countries, policies and rules adopted may be part of a strategy put in place by governments to ensure a "cyber-sovereignty" over the digital economy and society. In such cases, legal requirements are sometimes accompanied by rules on data localization, in application of which data must remain on the national territory and be processed locally.

The rationales underlying these national policies are translating into various restrictions to the flow of data beyond a country's border. Such restrictions may act as protectionist measures. Online privacy policies create a "new generation" of non-tariff barriers to digital trade, and damage trust in the digital economy. For example, measures to restrict cross-border data flows could:

- hamper e-commerce by limiting international online payments;
- impede global supply chains seeking to use blockchain to track products or manage supply chains, customs documentation, or electronic payments;
- block companies from using cloud computing to aggregate and analyze global data, or from gaining economies of scale;
- constrain the trading of crypto-currency; or
- limit the use of advanced technology like artificial intelligence.

In parallel, the requirement of data localization in the country (i.e., requiring organizations to store data on local servers) causes the obligation for foreign businesses to set up data centers locally, thus involving duplication, high cost and need for expertise. It is not surprising, therefore, that a recent study on U.S. companies pointed out that data localization rules are the most-cited digital trade barrier (U.S. International Trade Commission, August 2017).

Divergent national privacy approaches entail an increasing legal uncertainty and raise the costs of doing business. In a context of geographical fragmentation of the Internet, multinational companies roll out various action plans. One response is to abandon the company's investment or expansion plans in jurisdictions where it is difficult to move data in and out of the country. Other companies also move out of countries where data protection is too lax that they risk being non-compliant with their own home countries' data protection policies. Another response is to decide to duplicate their cost by building redundant data centers to comply with data localization or stringent data flow restrictions. This latter case is likely possible only for bigger markets but not for smaller economies (Pasadilla, 2020).

III -Fragmented and Inadequate National and International Regulatory Frameworks

While global economy evolves towards an information network, the regulation of cross-border data flows remains cacophonic.

A large number of countries, in particular developing economies, do not have data protection and privacy laws, since less than 130 countries have, so far, adopted such regulations or are in the process of enacting an equivalent law. In Africa, for example, less than 45% of countries have adopted legislation in this area, and in Oceania no country has legislated on data protectionto date. As a result, UNCTAD has estimated at more than 400 million the number of Facebook users residing in countries where data is not protected by law (UNCTAD Secretariat, 2019). To justify this situation,

these countries invoke their low level of technological development, a weak expertise in this field, but also the loss of competitiveness of their companies in terms of costs and organizational burden.

For countries having decided to regulate cross-border data transfer, several types of legal frameworks are available: 1) data protection and privacy law; 2) cybersecurity law; or 3) other digital trade policies (i.e. digital taxation…). Irrespective of the legal framework, countries vary in their privacy policies and laws, reflecting differing priorities, cultures, and legal structures.

In addition to the differences in objectives mentioned above, there are variables regarding the formulation of national legislations. Certain regimes (called "general schemes") apply uniformly to all those involved in the processing of personal data. Other regimes provide specific rules for certain industries (for example, health), certain types of entities processing data (for example, public authorities) or certain categories of data (for example, data relating to children). They do not foresee any regulatory control for other sectors.

A distinction can also be made between regimes which are essentially based on enforcement procedures initiated by individuals or groups representing them, and those which entrust enforcement powers to a specialized supervisory body, responsible for continuously monitoring the behavior of those who process personal data.

The imbroglio at the international level is exacerbated by variable definitions and interpretations given by national legislations and jurisprudence on what is considered "personal" "sensitive" or "important" or "strategic" information; as well as by differing deterrence and sanction systems among countries.

According to ECIPE's Digital Trade Restrictiveness Indexh, China is the most restrictive digital trade country among 64 countries surveyed, followed by Russia, India, Indonesia, and Vietnam ("DTRI Trade Restrictiveness Index," April 2018). The U.S. ranks 22 in the index, less restrictive than Brazil or France but more restrictive than Canada or Australia (the index ranks individual countries and does not rank the EU as a single unit). The relatively high U.S. score largely reflects financial sector restrictions. The "restrictions on data" category covers data policies such as privacy and security measures; this category is included in the composite index. Looking specifically at the 64 countries' data policies, Russia is the most restrictive country, followed by Turkey and China. Russia's policies include data localization, retention, and transfer requirements, among others. In contrast, the United States ranks 50 for data policy restrictions.

Regulatory restrictions affecting digital services have been confirmed in 2018 by the OECD's Digital Services Trade Restrictiveness Index (Digital STRI). The latter emphasized that digital services trade restrictiveness level may vary across States by referring on cross-cutting barriers that affect all types of services traded digitally across five broad categories, namely infrastructure and connectivity, electronic transactions, payment system, intellectual property rights, and other barriers affecting trade in digitally enabled services.

As a rule, OECD member economies like EU countries, Japan, Republic of Korea, and Australia have more liberal policies with respect to cross-border data transfer

if the recipient country has substantially similar data protection regime, adheres to similar privacy principles, safeguards are put in place for third party receivers of data (including through contracts), and individuals consent to the data transfer. There are some variations on data considered as sensitive that require more stringent regulations.

A brief snapshot of top global trading nations shows that the US, the UE and China, have designed their data policies from different perspectives. The EU's policies are driven by privacy concerns, considering the privacy of communications and the protection of personal data to be fundamental human rights, which are codified in EU law (CRS Report, 2020). The GDPR is perceived as "[…] the most comprehensive, high standard data protection law with wide reaching implications for many companies in and outside of the EU" (Pasadilla, 2020). Its salient features include:

- *Individual-centric provisions (mandating individual consent for the collection, storage, use, processing, transfer of personal data; right to be forgotten, data portability);*
- *Controller-processor model of data protection regulation with an independent data protection authority that can impose huge fines and penalties for non-compliance up to four percent of annual global turnover or 20 million euro (whichever is higher);*
- *Extra-territoriality of its applications;*
- *limited transfer of personal data in or out of the EU to specific Binding Corporate Rules (BCRs) or Model Contracts approved by the EU. Granting trade partners "adequacy" status for personal data transfers is also possible, which means that the EU has deemed that a country's laws and regulations provide an adequate level of data protection; currently, fewer than 15 jurisdictions are deemed adequate by the EU.*

Adopting a more pragmatic and balanced position, the US approach displays some special features: 1) while the US has traditionally sought a balanced approach between trade, privacy and security, the ultimate priority of free flow of data is to maintain open commerce and preserve US high tech companies' competitiveness; 2) data-specific approach regulating data privacy, with laws protecting specific information, such as healthcare or financial data; ; 3) State-level privacy policies, creating a patchwork of diverse state requirements and enforcement authorities.

China's data protection policies are contained in its consumer protection laws, cybersecurity laws and sector-specific laws. China's policies are based on national security justifications; China's trade and internet policies reflecting state direction and industrial policy, limiting the free flow of information and individual privacy.

In sum, differing national privacy approaches raise the costs of doing business by increasing compliance costs for organizations that function in multiple states, and may restrict international trade and commerce as a company based in one state may decline to serve a customer across state lines due to the complexity of complying with different or conflicting data requirements.Divergent national privacy laws make also it harder for governments to collaborate and share data, whether for scientific research, defense, or law enforcement.

IV- Shaping a global approach balancing policy objectives

For stakeholders and national governments the challenge consist in booming digital trade, while building trust in digital economy by reaching a global consensus based on a balance between three requirements: 1) ensuring effective personal data and privacy protection; 2) promoting a better global interoperability between different national systems, minimizing costs and allowing entities in different jurisdictions with varying online privacy regimes to share data via cross-border flows; and 3) taking into consideration variable public policy priorities.

Shaping a more appropriate approach means working concurrently at national, bilateral, regional and multilateral fora.

At the national level, expanding GDPR beyond the EU could be a step forward. Some experts contend that the GDPR may effectively set new global data privacy standards, since many companies and organizations are striving for GDPR compliance to avoid being shut out of the EU market, fined, or otherwise penalized, or in case other countries introduce rules that imitate the GDPR (Jesdanum, 2018). The regulatory inspiration from the GDPR is already reflected in dozens of countries, particularly in French-speaking countries such as Morocco, Tunisia, Benin, Mali, Canada and Switzerland. A number of other countries, including Brazil, India, Japan and the Republic of Korea, have adopted similar policies.

But it is quickly forgotten that exporting personal data under EU GDPR remains a daunting task since it is permitted in a restricted list of cases, and that, for example, the way the EU grants trade partners "adequacy status" for personal data transfers could be accused of being obscure and inconsistent, making them vulnerable to legal challenges. The extraterritorial approach and the risk of possible tensions with partners, as well as the European cultural and constitutional approach underlying privacy and data protection are also difficult to be transposed into other legal systems.

Divergent States' approaches mentioned above, as well as the gaps specific to each domestic legislation, do not clearly allow the spread of a single system on an international scale. To strengthen harmonization and interoperability between national privacy policies, bilateral FTAs can play a crucial role. But this path is not yet unanimously agreed upon.

Numerous organizations defending consumer interests and fundamental rights and freedoms in the digital environment, mainly in the EU, underscore that personal data and privacy are weakened by trade agreements. The European Consumer Organization (BEUC), the European Digital Rights (EDRi), or even the Centre for Digital Democracy (CDD) see an inherent conflict between online security, privacy, and trade. Trade and privacy would be complicated bed fellows. For them, it is unacceptable that, for example, the EU's privacy and data protection rules could be challenged through trade policy. Trade deals should not undermine consumers' fundamental rights and their very trust in the online economy. They point out that "[…] *the United States is aggressively pushing for a trade deal with the EU that would permit the unprecedented expansion of commercial data collection, threatening both consumers and citizens. America's data giants, such as Google and Facebook, want the TTIP to serve as a digital `Trojan Horse' that effectively sidesteps the EU's human-rights-based data protection*

safeguards" (Chester, 2016).

Despite EU leaders' commitmentsto safeguard people's rights to privacy and data protection in trade agreements by ensuring high standards for fundamental rights, these organizations have proposed to incorporate the following guarantees and safeguards into the current EU policy:

1)Keeping rules on privacy and data protection out of trade agreements, by means of a legally-binding exclusion clause, with an exception that allows any signatories to regulate cross-border data transfer in any sector that deals with the processing and transfer of personal data, such as financial services, within a trade agreement. Such a position would be in line with the European Parliament's call (Resolution of 3 February 2016, 2015/2233 (INI), parag (c)).

2) Preventing clauses in trade agreements which would oblige the signatories to submit forthcoming rules on privacy and data protection to a "trade test" in order to see if they are more burdensome than necessary.

3) Requiring from national data protection commissions or authorities to issue an opinion on the texts of free trade agreements.

However, this approach sounds to be isolated on a global scale. The tendency of States and businesses is to consider that policies balancing cross-border data flows, which often include personal data, with online privacy and securitycan be coherent and consistent. Modern trade agreements increasingly include provisions which allow unrestricted transfers of data between countries, including personal data.

US and EU FTAs have sought to cover a broad range of measures to liberalize bilateral trade with partner countries, including the reduction of tariffs and provisions on services, technical barriers to trade, intellectual property and, most recently, ambitious provisions addressing potential digital barriers to trade. The U.S. government has traditionally sought to balance these objectives.Recent free trade agreements translate the U.S. position into binding international commitments. The EU's trade negotiators claim that present and future trade deals will not undermine data protection and privacy rights. By defending consumer interests and fundamental rights and freedoms in the digital environment, the European negotiators ensure that personal data and privacy are not weakened by EU trade agreements.

To succeed, this approach shall be pragmatic, consensual and balanced. For this purpose, expanding "OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" (OECD Privacy Guidelines) beyond Members could represent the next step toward consistent international rules and disciplines on data flows and privacy. Any national privacy policy or international agreement should be based on the following three pillars:

1) Adopting data protection principles and standards in accordance with OECD Privacy Guidelines, as revised in 2013, which would constitute the foundation on which any regulatory framework should be built.
2) Setting up effective mechanisms for cooperation between national data protection commissions or authorities;
3) Ensuring a free flow and localization of data between countries, while recognizing that sometimes measures are necessary to achieve legitimate policy objectives such as consumer protection, privacy protection or national security and, in this

case, such measures should be the least trade restrictive, nondiscriminatory, and transparent.

Such a comprehensive approach enables a combination between the development of high common standards for data between countries and the introduction of a "trade test" founded on the WTO's guiding principles.

The OECD Privacy Guidelines are high-level policy recommendations that can be used as a basis to develop a privacy protection framework with the flexibility to accommodate regional and local variations. Meanwhile, they should facilitate international interoperability for cross-border flows of personal data.

For reminder, under OECD Privacy Guidelines:

1) Personal data collection should be
- lawful, fair, and with the consent of the individual;
- accurate, complete, up-to-date; and
- limited to fulfill the specified purpose.
2) Personal data processing should
- not be disclosed or made available without consent or by legal authority;
- be protected by security safeguards; and
- be available for establishing existence, nature, and purpose.
3) Individuals should have the right to access personal data collected and challenge data to correct, amend, or delete.
4) Data controller should be accountable for compliance.

A system for global interoperability in a least trade-restrictive and non-discriminatory way between different national systems could help minimize costs and allow entities in different jurisdictions with varying online privacy regimes to share data via cross-border data flows. Such a system could help avoid fragmentation of the internet between European, Chinese and American spheres, a danger that some analysts have warned against (The New York Times, October 15, 2018).

The OECD Guidelines have already inspired most regional conventions, recommendations and standards for privacy and data protection, including the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108, of 1981), the United Nations Guidelines concerning Computerized Personal Data Files (UN, 1990), the Asia-Pacific Economic Co-operation (APEC) Privacy Framework (APEC, 2005), the APEC Cross-Border Privacy Rules (CBPR, 2011), the International Standards on Privacy and Data Protection (Madrid Resolution, 2009). More recently, the Organization of American States' Model Law on Data Protection (OAS, 2014), the 2018 G-20 Digital Economy principles, CPTPP, USMCA, and the planned US-EU agreement (TTIP) provisions demonstrate an evolving understanding on how to balance cross-border data flows, security, and privacy, to create interoperable policies that can be tailored by countries and avoid fragmentation or the potential exclusion of other countries or regulatory systems. At the bilateral level, recent EU/Canada, EU/Japan and EU/Vietnam FTAs, as well as the future US/Kenya and US/UK agreements, confirm this pattern.

Some States have even moved one large step further in concluding agreements entirely devoted to digital economy's challenges. On March 23, 2020, Singapore and Australia have announced the conclusion of negotiations for the Singapore-

Australia Digital Economy Agreement (DEA). The latter is consistent with the Digital Economy Partnership Agreement (DEPA) signed between Singapore, Chile and New Zealand earlier this year. Through these agreements, Signatories seek to create an over-arching framework for deeper cooperation in the digital economy "[…] *to shape international rules, establish interoperability between digital systems and address frontier issues from emerging technologies*" (Joint Press Release, 23 March 2020). Key Features of these agreementscover various components, including artificial intelligence, data innovation, digital identities, cybersecurity, data flow, and trade facilitation.Under these agreements, Signatories thus undertaketo promote the APEC Cross Border Privacy Rules (CBPR) system, which goesbeyond OECD Privacy Guidelines, and to facilitate seamless data flows and prohibit data localization, subject to limited statutory exceptions.National data protection authorities are also committed to working closely to coordinate and provide mutual assistance in joint investigations involving cross-border personal data incidents.

Ultimately, the various trade agreements and initiatives with differing sets of parties may pave the way for a broader multilateral understanding and eventually lead to more enforceable binding commitments founded on the key WTO principles of non-discrimination, least trade restrictiveness, and transparency.

To date, there are no comprehensive multilateral rules specifically about privacy or cross-border data flows. WTO Agreements, including the General Agreement on Trade in Services (GATS), do not match current issuessince they are predating the current reach of the Internet and the explosive growth of global data flows, while many digital products and services that did not exist when the agreements were negotiated are not covered (Burri, 2017).

Yet that did not prevent the United States and other countries from addressing these issues within the WTO forum. The challenge is to reach an agreement between the 164 members of the World Trade Organization which was initiated in 2011 but which drags on, given the fact that the subject of personal data protection is drowned in middle of a greater whole representing E-commerce. The latter includes electronic transactions, but also cybersecurity, source code transfers, personal data protection, data transfers, and customs duties on products purchased online. To further complicate the issue, some lesser-developed countries, including India, oppose commencement of these negotiations. For them, E-commerce agreement would not bridge the Digital divide among nations and people. Such an agreement promotes a form of globalization for the richest few and for them only. Developmental issues covered by the WTO Doha Round should, in their view, take precedence over a new set of negotiations on e-commerce matters. These members are concerned that they do not have the infrastructure needed to fully take advantage of the liberalization of digital trade.

In the absence of significant progress in this area, the WTO plurilateral framework has gradually appeared to be more appropriate. Efforts to update the multilateral agreement and discussions for new digital trade rules under the WTO Electronic Commerce Work Program stalled in 2017 (WTO General Council, December 1, 2017). In December 2017, a coalition of more than 70 WTO members accounting for 90% of global trade, including the EU, the United States, China and Japan agreed to "initiate exploratory work together toward future WTO negotiations on trade-related aspects

of electronic commerce (WTO, "Joint Statement on Electronic Commerce" December 13, 2017).
The group formally launched the "E-commerce initiative" in January 2019 (WTO, WT/L/1056, 2019). The official joint statement lists the United States and EU as participants, and also several developing countries such as China and Brazil. India stated it will not join, preferring to maintain its flexibility to favor domestic firms, limit foreign market access, and raise revenue in the future. The statement did not define the scope of any potential agreement. Negotiations are officially launched in March 2019. The EU's position is ambitious since it consists in the submission of a first text, largely inspired by the GDPR, accompanied by data localization measures (European Commission, Press Release Database, January 25, 2019). The U.S. Trade Representative's (USTR's) statement emphasized "[…] *the need for a high-standard agreement that includes enforceable obligations and creates strong, market-based rules in this area and reduces the barriers around the world that threaten to undermine the growth of the digital economy, including restrictions on cross-border data flows and data localization requirements*" (USTR, January 25, 2019).

Conclusions

In an increasingly data-driven global economy, the challenge for stakeholders and governments consists in ensuring free transfer and access to data and information that is essential for booming the digital economy, while safeguarding privacy and data protection for individuals and strategic interests of States.
This study has revealed thatcurrent national and international legal frameworks regarding the regulation of data transfers and protection of privacy remain flawed and fragmented. There are no comprehensive multilateral rules specifically about privacy or cross-border data flows. Countries vary in their privacy policies and laws, reflecting differing priorities, cultures, and legal structures. Differing national international and privacy approaches raise the costs of doing business by increase compliance costs for organizations that function in multiple States and may restrict international trade and commerce, as a company based in one state may decline to serve a customer across state lines due to the complexity of complying with different or conflicting data requirements. Divergent national privacy laws and policies also make it harder for governments to collaborate and share data, whether for scientific research, defense, or law enforcement.
As argued before, it is now critical to promote a pragmatic, balanced and concurrent approach in national, regional and international fora based on the promotion of a universal legal corpus and close cooperation between competent national authorities. To be effective, such an adequate regulatory framework implies, for decision-makers, taking into consideration the various concerns of public authorities, consumers and businesses, whether they relate to national security, privacy protection, circulation and ownership of data or economic development.
To succeed, a more global approach balancing policy objectives would enable interoperability between differing national regimes, thereby facilitating and removing discriminatory trade barriers to cross-border data flows. Any national privacy

policy or international agreement should be based on the following three pillars: 1) adopting data protection principles and standards in accordance with OECD Privacy Guidelines; 2) setting up effective mechanisms for cooperation between national data protection commissions or authorities; and 3) providing for a "trade test" that ensures free flows and localization of data between countries, while recognizing that sometimes measures are necessary to achieve legitimate policy objectives and, in this case, such measures should be the least trade restrictive, non-discriminatory, and transparent.

Such an approach promotesa combination between the development of high common standards for protection data between countries and the introduction of a "trade test" founded on the key WTO principles. Balancing public policy priorities and complying with WTO principles are essential prerequisites and a first step toward a legal instrument of universal scope in this field.

References

Bughin J. and Lund S., (2017), The Ascendency of International Data Flows, McKinsey Global Institute, available: https://www.mckinsey.com/mgi/overview/in-the-news/the-ascendancy-of-international-data-flows

Burri M., (2017), The Regulation of Data Flows Through Trade Agreements, in Law and policy in international business, 48(1), 407-448, available: https://www.researchgate.net/publication/319469193.

Chang A., (2018), The Facebook and Cambridge Analytica scandal, explained with a simple diagram, available: https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

Chester, J., (2016), Study Launch: the EU can achieve data protection-proof trade agreements, available: https://edri.org/study-launch-eu-can-achieve-data-protection-proof-trade-agreements/

Congressional Research Service (CRS) Report (2020), Data Flows, Online Privacy, and Trade Policy, available: https://crsreports.congress.gov/product/pdf/R/R45584

European Centre for International Political Economy (ECIPE) (2018), DTRI Trade Restrictiveness Index, available: https://ecipe.org/dte/dte-report/

European Commission (2019), 75 countries launch WTO talks on e-commerce, Press Release Database.

European Parliament (2016), Resolution of 3 February 2016 containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA), 2015/2233(INI).

Greenlaaf, G., (2018), Asia-Pacific Free Trade Deals Clash with GDPR and Convention 108, Privacy Laws & Business International, Report 22-24.

Jesdanum, A., (2018), Microsoft pledges to extend EU data rights worldwide, available: https://www.foxbusiness.com/features/microsoft-pledges-to-extend-eu-data-rights-worldwide

Joint Press Release (23 March 2020), Singapore Concludes Negotiations for Digital Economy Agreement with Australia,available: https://www.mti.gov.sg/-/media/MTI/Newsroom/Press-Releases/2020/03/Joint-press-release--Conclusion-of-Negotiations-for-the-SingaporeAustralia-Digital-Economy-Agreement.pdf

MicKinsey Global Institute (2016), Digital Globalization: the new Era of Global Flows, available:https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows

Pasadilla, G., (2020), Next Generation Non-Tariff Measures: Emerging Data Policies and Barriers to Digital Trade, UN, ESCAP Working paper.
Sonmez, M., (2020), How personal data could help contribute to a COVID-19 solution, World Economic Forum.
The New York Times (October 15, 2018), Editorial Board, There May Soon Be Three Internets. America's Won't Necessarily Be the Best.
U.S. International Trade Commission (2017), Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions, Investigation Number: 332-561.
UNCTAD Secretariat (2019), The value and role of data in electronic commerce and the digital economy and its implications for inclusive trade and development, TD/B/EDE/3/2.
USTR (2019), USTR Robert Lighthizer on the Joint Statement on Electronic Commerce.
WTO (2019), Joint Statement on Electronic Commerce, WT/L/1056.
WTO,World Trade Report 2018: The future of world trade, available: https://www.wto.org/english/res_e/publications_e/wtr18_e.htm).
WTO General Council (December 1, 2017), Work Programme on Electronic Commerce, Report by the Chairman, WT/GC/W/739.
WTO (December 13, 2017), Joint Statement on Electronic Commerce,WT/MIN(17)/60.
Yoffie, D., Gawer, A., and Cusumano, M., (2019), "A Study of More Than 250 Platforms Reveals Why Most Fail", Harvard Business Review, available: https://hbr.org/2019/05/a-study-of-more-than-250-platforms-reveals-why-most-fail